جبر

نوشتهٔ

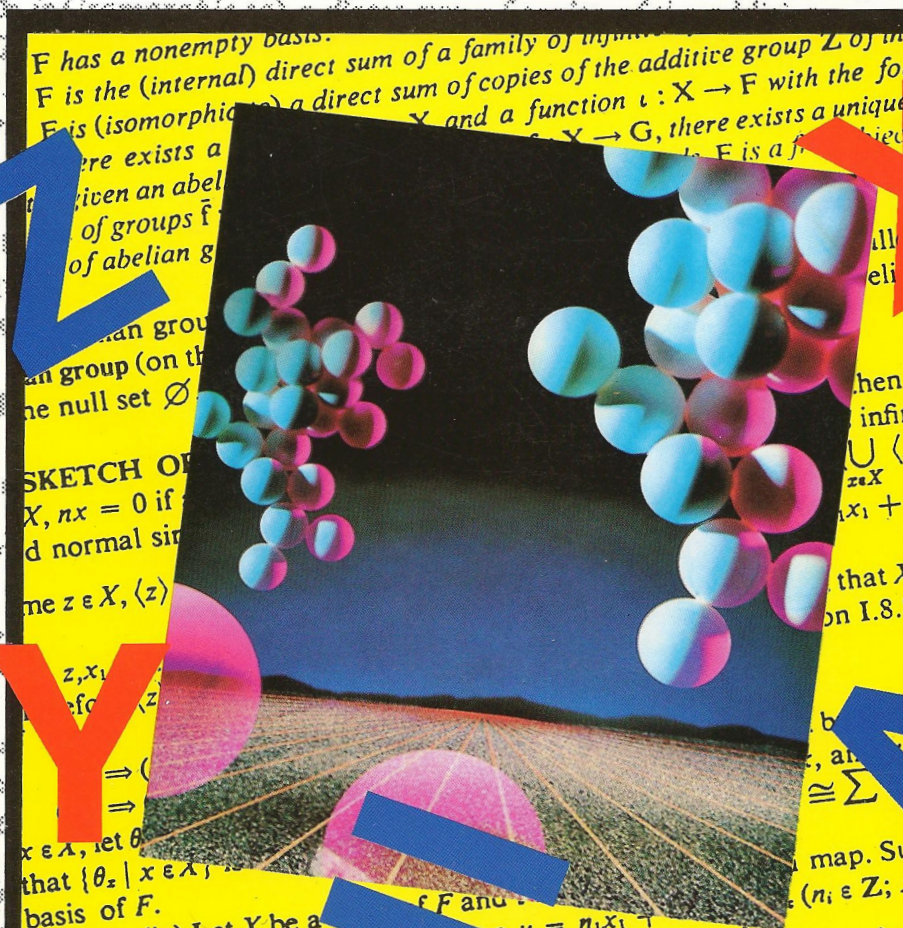
توماس دبلیو . هانگر فورد

ترجمهٔ

دکتر علی اکبر عالم زاده دکتر حسین ذاکری

Algebra

Thomas.W.Hungerford



جبر

نوشتهٔ

توماس دبلیو. هانگرفورد

ترجمهٔ

دکتر علی‌اکبر عالم‌زاده

دکتر حسین ذاکری

پیشگفتار مترجمان

همانطور که از پیشگفتار مؤلف بر می‌آید، این کتاب برای سال اول فوق لیسانس نگاشته شده است. ترجمهٔ کتب بالاتر از لیسانس همیشه مورد ایراد اهل فن بوده است. برخی از استادان برگردان این نوع کتب را سودمند نمی‌دانند و دلیلشان این است که دانشجوی بالاتر از لیسانس باید با زبان بیگانه ادامهٔ تحصیل دهد وخود را برای استفاده از منابع جهانی آماده سازد؛ لذا، ترجمهٔ این نوع متون وی را از راه اصلی منحرف می‌سازد. از آن سو، ناشران از چاپ کتب فوق لیسانس که خوانندهٔ کمی دارد به دلیل اقتصادی سرباز می‌زنند. ما ایران مردان که همه چیزمان زبان ماست و تعهدی نسبت به زبان بیگانه نداریم اولین ایراد را حرف قابل اعتنایی نمی‌دانیم. اما بحث اقتصادی ناشران نکتهٔ قابل تأملی است که باید بدان توجه کرد. کتاب یک کالای فرهنگی - اقتصادی است که عدم توجه به هر جنبه‌اش آن را با شکست مواجه می‌سازد. خوشبختانه زمانی این کتاب به چاپ می‌رسد که بخش اعظمی از مطالب آن به دورهٔ لیسانس کشیده شده است. این امر به خاطر ارتقاء حیرت آور سطح ریاضی دانشگاههای کشور است که این خود تقریباً مدیون ترجمهٔ کتب ریاضی در سالهای اخیر می‌باشد. ما این کتاب راکه برای فوق لیسانس نگاشته شده است با کمال افتخار به دورهٔ لیسانس تقدیم می‌داریم.

دکتر علی‌اکبر عالم‌زاده

دکتر حسین ذاکری

گروه آموزشی ریاضی

دانشگاه تربیت معلم

پیشگفتار مؤلف بر ویرایش اشپرینگر

استقبال از ویرایش اول این کتاب حاکی از آن بود که این متن یک جلدی و خود کفا جبر لازم در سطح فوق لیسانس است که برای دانشجوی متوسط در این سطح خواندنی بوده و نیاز مدرسین و دوره‌های مختلف تدریس را برمی‌آورد. این استقبال بیانگر آن بود که کتاب فعلاً اصلاحات وسیعی را طلب نمی‌کند. لذا، در این ویرایش تغییری اساسی داده نشد. لیکن تمام غلطهای چاپی و اشتباهات معلوم شده اصلاح و چند برهان بازنویسی شدند.

مایلم از پل هالموس (Paul Halmos) و اف.دبلیو.گرینگ (F.W. Gehring) و نیز کارکنان مؤسسهٔ اشپرینگر به خاطر ترغیب و یاریشان در این چاپ تشکر نمایم. مایهٔ خشنودی است که این کتاب مدام در اختیار جامعهٔ ریاضیدانان قرار خواهد داشت. از آنجا که بسیاری از ناشران در پی چاپ کتبی یا کیفیت پایین ولی سود بیشترند، لازم است مؤسسهٔ اشپرینگر - فرلاگ (Springer - Verlag) را به خاطر تمایل به چاپ کتب ریاضی با کیفیت بالا ستود.

توماس دبلیو. هانگرفورد
سیتل، واشنگتن
ژوئن ۱۹۸۰

تذکر در باب چاپ سوم. در این چاپ غلطهایی اصلاح شدند که آنها را مرهون چشمان تیزبین جرج برگمن (George Bergman) در برکلی و ککین فنک (Keqin Feng) از دانشگاه علوم و صنعت چینی می‌دانم.

پیشگفتار مؤلف

تذکر. بحث کامل طرق استفاده از این کتاب همراه با خلاصه‌ای از درسهای پیشنهادی در صفحهٔ خ مطرح شده است.

این کتاب متنی است برای درس جبر در آغاز دورهٔ فوق لیسانس. نگارش آن سالها پیش و در زمانی شروع شد که کتابی یک جلدی و مناسب برای این دوره وجود نداشت. خصلتهای "مناسب بودن"، که امید است این کتاب از آنها بهره‌مند باشد، به قرار زیرند.

(یک) کوشیده‌ام کتاب چنان باشد که یک دانشجوی فوق لیسانس متوسط (ولی تا حدودی آماده) بی مشکل آن را بخواند. تأکید بیشتر روی وضوح بوده است تا اختصار.

(دو) برای راحتی خواننده کتاب اصولاً خودکفاست. لذا، مطالب زیادی از سطح لیسانس را شامل است که خوانندهٔ آماده می‌تواند به سهولت آنها را حذف نماید.

(سه) از آنجاکه مواد جبر سال اول فوق لیسانس مورد توافق عام نیست، درکتاب مطالبی بیش از یک سال گنجانده شده است. همچنین مباحث اصلی سال اول فوق لیسانس با وسعت و عمق کافی مطرح شده‌اند. متأسفانه، رعایت جا و صرفه‌جویی موجب حذف برخی از مباحث، مانند نظریهٔ ارزیابی، گردیده‌است.

در اکثر موارد مجالی برای تدریس این مطالب حذف شده در یک درس یکساله باقی نخواهد ماند.

(چهار) کتاب به نحوی تدوین یافته که مدرس بیشترین انعطاف را در انتخاب، ترتیب، و میزان

تدریس مواد (بدون فدا شدن جذابیت مطلب برای دانشجو) خواهد داشت.

(پنج) تعداد تمرینات به نحوی غیرمعمول زیاد است.

به طور نظری هیچ پیشنیاز رسمی جز چند مطلب مقدماتی در باب مجموعه‌ها، تابعها، اعداد صحیح، و اعداد حقیقی و کمی "پختگی ریاضی" وجود ندارد. ولی عملاً یک درس جبر مدرن در سطح لیسانس احتمالاً برای اغلب دانشجویان لازم خواهد بود. در واقع کتاب با این فرض نگاشته شده است. لذا، چند مفهوم که دانشجوی فوق لیسانس باید با آنها آشنا باشد (مثلاً ماتریسها) در مثالها، تمرینات، و برهانهای اتفاقی پیش از مطرح شدن صوری آنها در متن عرضه خواهد شد.

فلسفهٔ اصلی کتاب آن است که مطالب با ***بیشترین عمومیت قابل استفاده که با آموزش مناسب سازگار است*** ارائه شوند. اعمال این اصل در مسائل مختلف تکنیکی نسبتاً آسان است. لیکن کاربردش در مسائل وسیعتر با ساختار مفهومی مشکلتر می‌باشد. از یک سو، مثلاً، شاگرد باید از دیدگاههای نسبتاً جدید در ماهیت جبر آگاه شود: در حال حاضر اصل مطلب مطالعهٔ ریختها (نگاشتها) است؛ بسیاری از مفاهیم عمیق و مهم به صورت خواص نگاشت عمومی به بهترین وجه مجسم می‌شوند. از سوی دیگر، سطح عالی تجرید و تعمیم را فقط کسانی کاملاً درک می‌کنند که زمینهٔ مناسبی در حالات خاص که این تجریدها را موجب شده‌اند دارند. لذا، در صورت وجود تعریفی آشناتر یا قابل درک تر، مفاهیم قابل توصیف با خاصیت نگاشت عمومی توسط این خاصیت ***تعریف*** نمی‌شود. در این حالات، خاصیت نگاشت عمومی در یک قضیه داده خواهد شد.

رسته‌ها به سرعت معرفی شده و سپس چند ***اصطلاح*** از این نظریه کراراً به کار رفته‌اند. لیکن، زبان رسته‌ها عمدتاً به عنوان یک ابزار تسهیل به کار خواهد رفت. خوانندهٔ ناآشنا با رسته‌ها در اکثر بخشهای کتاب (حتی به عنوان مرجع) مشکلی نخواهد داشت. با اینحال، مدرس علاقه‌مند می‌تواند با تدریس زودتر فصل ده (رسته‌ها) به آسانی به درس خود رنگ و بوی رسته را بیفزاید. چون این فصل اساساً از بقیهٔ کتاب مستقل است، آن را می‌توان در هر زمان مطالعه کرد.

ویژگیهای ریاضی دیگر کتاب به قرار زیر است.

مجموعه‌های نامتناهی، اعداد اصلی نامتناهی، واستدلالهای ترانسفینی به طور اصولی به

کار رفته‌اند. تمام پیشنیازهای ما از نظریهٔ مجموعه‌ها به انضمام برهانهای کاملی از مطالب مربوطه در حساب اعداد اصلی در فصل آشنایی داده شده است.

برهان قضایای زیلوف (Sylow) که توسط آر.ج.نونکه (R.J.Nunke) داده شده است نکاتی را که اغلب برای بسیاری از دانشجویان مبهم است روشن خواهد ساخت.

بحث ما از نظریهٔ گالوا (Galois) از آن ایروینگ کاپلانسکی (Irving Kaplansky) است که برخی از ایده‌ای امیل آرتین (Emil Artin) رابا موفقیت بسط داده است. گروه گالوا و ارتباط اصلی بین زیر گروهها و زیر میدانها در محدودهٔ یک جفت میدان کاملاً کلی تعریف شده‌اند. این، همراه با چیزهای دیگر، به ما اجازهٔ تعمیم آسانی از نتایج مختلف به حال ابعاد نامتناهی را خواهد داد. قضیهٔ اساسی در آغاز، پیش از معرفی میدانهای تجزیه‌گر، نرمالی، جدایی پذیری، و غیره، ثابت شده است. در نتیجه، خطر واقعی، یعنی عدم رؤیت جنگل به خاطر درختانش، مینیمم شده و یا احتمالاً از بین رفته‌است.

ما در توسیعهای میدان جدایی پذیر حالات جبری و متعالی را از هم جدا می‌سازیم. این امر از دیدگاه آموزشی به مراتب از روش بورباکی (Bourbaki) که ارائه همزمان دو حالت است بهتر خواهد بود.

هرگاه فرض کنیم همهٔ حلقه‌ها یکدار باشند، تمام همریختیها واحدها را حفظ کنند، و همهٔ مدولها نیز یکدار باشند، آنگاه می‌توان حلقه‌ها و مدولهای نیمه ساده را به سرعت مطرح کرد. متأسفانه این روش شاگرد را برای بسیاری از مطالب نظریهٔ حلقه‌های تعویض ناپذیر آماده نمی‌سازد. در نتیجه، نظریهٔ ساختاری حلقه‌ها (بخصوص، حلقه‌های آرتینی چپ نیمه ساده) در محدودهٔ کلیتری مطرح شده است. این بحث وضعیت فوق‌الذکر را شامل شده ولی به حلقه‌های فاقد یک، رادیکال ژاکوبسون (Jacobson) و مباحث مربوطه نیز به طور کامل خواهد پرداخت. به علاوه، رادیکال اول و قضیهٔ گولدی (Goldie) در حلقه‌های نیمه اول نیز مطرح خواهند شد.

تمرینات زیادی با دیدگاه و میزان سختی متفاوت داده شده‌اند. تجربهٔ من در "ستاره‌دار کردن" تمرینهای مشکلتر دلیلی است بر صحت این ضرب‌المثل قدیمی که می‌گوید: گوشت تن هر کس سمّی است برای دیگری. لذا، هیچ تمرینی را ستاره‌دار نکرده‌ام. تمرینات از آنجهت مهم اند که اگر شاگرد تعداد مناسبی از آنها را حل نکند درک یا تسلط کاملی بر مطالب نخواهد داشت. اما

تمرینات بخش کاملی از متن را تشکیل نمی‌دهند بدین معنی که برهانهای غیر بدیهی برخی از نتایج لازم کاملاً به عنوان تمرین گذارده شده است.

بااینحال، بسیاری از شاگردان، در صورت راهنمایی شدن، قادر به اثبات احکام غیر بدیهی می‌باشند. در نتیجه، بسیاری از قضایای متن به جای برهان کامل فقط با "طرح برهان" مزین شده‌اند. گاهی این طرح چیزی جز ارجاع به قضایای مناسب نیست. در حالات دیگر، این طرح بخشهای مشکلتر برهان یا "ترفند" لازم را کاملاً شرح داده و بقیهٔ کار را حذف کرده است. اغلب تمام مراحل مهم یک برهان بیان شده و دلایل یا جزئیات محاسبه‌ای عادی به خواننده محول شده‌است. بسیاری از افراد بعضی از "طرحها"ی نوع اول را برهان کامل می‌دانند. در این حالات، واژهٔ "طرح" به شاگرد این هشدار را می‌دهد که برهان مورد نظر به نوعی خلاصه شده و درکش از برخی برهانهای "کامل" در متن آسانتر نیست.

توماس دبلیو. هانگرفورد
سیتل، واشنگتن
سپتامبر ۱۹۷۳

تشکر و قدردانی

درنگارش این کتاب افراد بسیاری به طور مستقیم یا غیرمستقیم نقش داشته‌اند. پیش از همه از چارلز کانوی (Charles Conway)، وینسنت مک برین (Vincent McBrien)، ریموند سوردز، اس. ج. (Raymond Swords, S.J)، و پل هالموس (Paul Halmos) سپاسگزارم که اگر تذکرات، تشویقات، و یاری آنان در مراحل مختلف تحصیلی من نبود هرگز ریاضی‌دان نمی‌شدم. همچنین از استاد راهنمای رساله‌ام ساندرز مک لین(Saunders MacLane) تشکر دارم که اولین رهنمون من در هنر نگارش ریاضی بوده است. تنها امید آن است که این کتاب به کتب عالی و باکیفیت بالای وی نزدیک شده باشد.

همکارانم در دانشگاه واشنگتن نظراتی در بخشهای مختلف دستنویس ابراز داشته‌اند. بویژه، از آر.ج.نونکه (R.J. Nunke)، جی.اس. مونک(G.S. Monk)، آر. وارفیلد(R. Warfield)، و دی. کنودسون(D. Knudson) سپاسگزارم، همچنین از دانشجویانی که صورتهای مقدماتی دستنویس را در چهارسال گذشته مورد استفاده قرار داده‌اند تشکر می‌نمایم؛ نظرات آنها موجب اصلاحات زیادی در نتیجهٔ نهایی شده است.

همچنین خدمات تایپی دانشگاه واشنگتن را از صمیم قلب ارج می‌نهم. دو صورت مقدماتی دستنویس توسط دونا تامپسون (Donna Thompson) تایپ شد و در این راه افرادی چون یان نی(Jan Nigh)، پت واتانابه (Pat Watanabe)، پام برینک(Pam Brink)، و ساندرا ایوانز(Sandra Evans) یاری داشته‌اند. صورت نهایی دستنویس به وسیلهٔ سونجااگل (Sonja Ogle)، کی کولودزیج مارتین(Kay Kolodziej Martin)، و ویکی کاریل

(Vicki Caryle) و گهگاه با کمک لویی بوند (Lois Bond)، گری بوتون (Beri Button)، و یام شیل (Jam Schille) تایپ شده است.

همسرم ماری (Mary) به خاطر شکیبایی اش در زمان (به ظاهر نامحدود) نگارش این کتاب شایستهٔ تقدیر است. آخرین کلام راجع به دختر سه ساله‌ام آن (Anne) و پسر دوساله‌ام تام (Tom) است که تولد غیره منتظره‌شان پس از یازده سال ازدواج نگارش این کتاب را طولانی ساخت، که البته بهای کمی است برای این چنین فرزندان.

نکاتی راجع به استفاده از این کتاب

اطلاعات عمومی

در یک بخش، همهٔ تعریفات، لمها، قضایا، احکام، و نتایج شمارهٔ متوالی دارند (مثلاً، در بخش ۳ از یک فصل، چهارمین فقره دارای شمارهٔ ۴.۳ می‌باشد). تمرینات هر بخش با سیستم جداگانه‌ای شماره‌دار شده‌اند و مراجع مخلوط طبق طرح زیر اداره می‌شوند.

(یک) بخش ۳ از فصل پنج در سراسر فصل پنج به صورت بخش ۳ و در جاهای دیگر به صورت بخش ۳.۷ ارجاع می‌شود.

(دو) تمرین ۲ از بخش ۳ در فصل پنج در سراسر بخش ۳.۷ به عنوان تمرین ۲، در سایر بخشهای فصل پنج به صورت تمرین ۳.۲، و در جاهای دیگر به صورت تمرین ۷. ۲.۳ نموده می‌شود.

(سه) چهارمین فقرهٔ شماره‌دار (تعریف، قضیه، نتیجه، حکم، یا لم) بخش ۳ از فصل پنج در سراسر فصل پنج به صورت فقرهٔ ۴.۳ و در جاهای دیگر به صورت ۷. ۴.۳ نموده خواهد شد.

پیش از واژه‌نامه، لیست کاملی از علایم ریاضی آمده است.

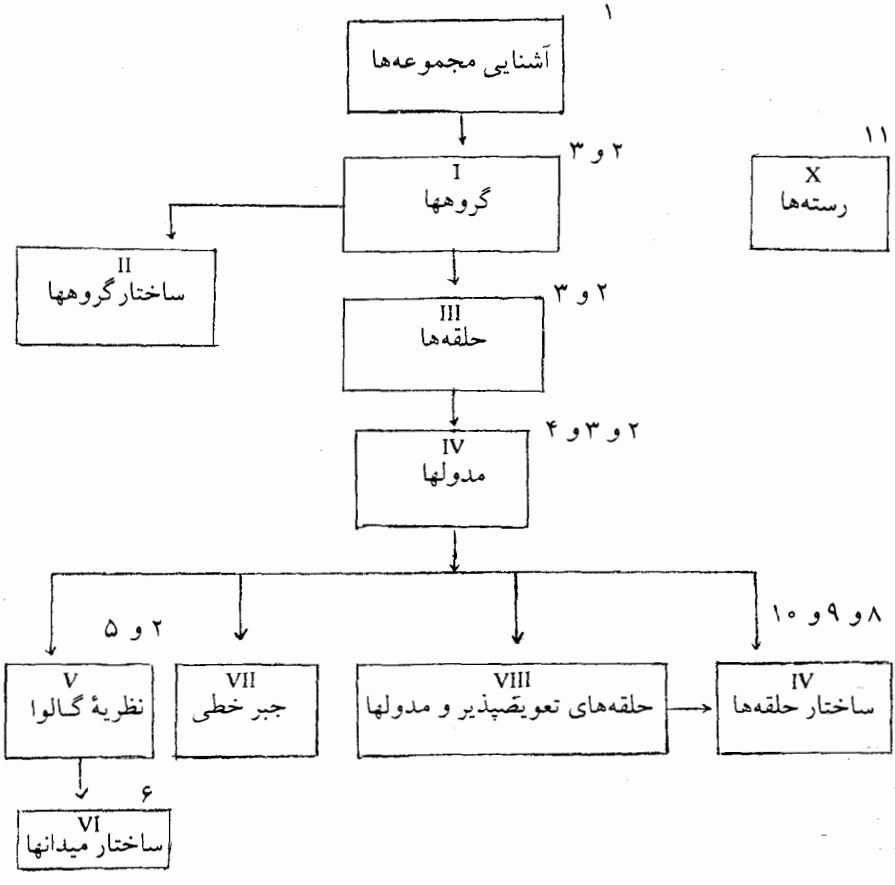
عبارت ***نعل به نعل*** تقریباً به این معنی است: "باتغییر دادن اشیاء که (بوضوح) باید تغییر کنند (تااستدلال در وضعیت حاضر برقرار و با معنی شود)".

در این کتاب واژهٔ "حکم" فقط به نتایجی اطلاق شده است که در آینده (جز در چند تمرین یا برهان "احکام" دیگر) به کار ***نمی‌روند***. در نتیجه، ***خواننده‌ای که بخواهد فقط خط اصلی کتاب را دنبال کند می‌تواند تمام احکام (و لمها و نتایج آنها) را بدون ایجاد مانع حذف نماید.*** لمها یا

قضایا تقریباً همیشه در جایی در آینده به‌کار خواهند رفت. اگر قضیه‌ای در یک یا دو مورد پس از اولین ظهورش لازم شود، این امر معمولاً ذکر خواهد شد. چند استثنا در این طرح شماره‌گذاری مشکل چندانی ایجاد نخواهد کرد.

ارتباط متقابل فصلها

جدول زیر ارتباط متقابل فصلها را نشان می‌دهد و لازم است همراه با فهرست مطالب و تذکرات زیر (که در بالای مستطیلها نموده شده‌اند) خوانده شود. به علاوه، خواننده برای اطلاعات بیشتر در باب ارتباط متقابل بخشهای مختلف یک فصل باید به مقدمهٔ آن فصل مراجعه نماید.



تذکرات

۱. بخشهای ۱ تا ۷ فصل آشنایی اساسی بوده و کراراً در آینده به کار می‌آیند. این مطالب جز بخش ۷ (لم زرن) تقریباً همه مقدماتی می‌باشند. همچنین شاگرد باید تعریف عدد اصلی را بداند (بخش ۸ تا تعریف ۴.۸). بقیهٔ بخش ۸ فقط پنج بار لازم خواهد بود (قضایای II. ۲.۱ و IV. ۶.۲؛ لم ۵.۳.V؛ قضایای V. ۶.۳ و VI. ۹.۱). حساب اصلی را می‌توان تا زمان نیاز به تعویق انداخت و یا به عنوان مطالعهٔ خارج به افراد علاقه‌مند توصیه کرد مگر آنکه شخص بخواهد وقت زیادی صرف آن نماید.

۲. دانشجویی که یک درس جبر مدرن دورهٔ لیسانس (یا معادل آن) راگذرانیده و با مطالب مذکور در فصل آشنایی آشناست بلافاصله می‌تواند از هر یک از فصلهای یک، سه، چهار، یا پنج شروع نماید.

۳. به خواننده‌ای که می‌خواهد از فصل یک چشم بپوشد قویاً توصیه می‌شود که با مرور بخش I. ۷ مطمئن شود که با زبان نظریهٔ رسته‌ها که در آنجا معرفی شده است آشناست.

۴. مواد لازم از فصل سه در فصل چهار جز در یک مورد تعاریف اصلی بخش III. ۱ است. لیکن بخش III. ۳ پیشنیازی است برای بخش IV. ۶.

۵. برای مطالعهٔ توسیعهای میدان رادیکال (بخش V. ۹) به اطلاعاتی از گروههای حلپذیر (بخشهای II. ۷ و II. ۸) نیاز خواهد بود.

۶. فصل شش فقط به شش بخش اول فصل پنج نیازمند است.

۷. برهان قضیهٔ صفرهای هیلبرت (بخش III. ۷) به معلوماتی از درجات تعالی (بخش VI. ۱) و نیز مطالب بخش V. ۳ محتاج است.

۸. بخش VIII. ۱ (شرایط زنجیری) به طور وسیعی در فصل نه به کار می‌رود، اما فصل نه از بقیهٔ فصل هشت مستقل است.

۹. ارتباط اصلی بین ماتریسها و در و نریختیهای مدولهای آزاد (بخش VII. ۱ تا قضیهٔ VII. ۴.۱) در بررسی ساختار حلقه‌ها به کار می‌رود (فصل نه).

۱۰. بخش V. ۳ پیشنیازی است برای بخش IX. ۶.

۱۱. بخشهای I. ۷، IV. ۴، و IV. ۵ پیشنیاز فصل ده می‌باشند؛ جز این، فصل ده اساساً از بقیهٔ

کتاب مستقل است.

خلاصه‌ای از درسهای پیشنهادی

اطلاعات فوق همراه با آشنایی با فصول گوناگون برای طراحی دروس مختلف با محتوا و زمان متفاوت کافی است. چند درس چهار ماهه (۳۰ وقت کلاسی) در مباحث گوناگون ذیلاً ذکر شده است.

این توصیفات بسته به مفروضات، سطح کلاس، و غیره تا حدودی قابل انعطاف اند. ما مطالب زمینه (اغلب با ماهیت مقدماتی) که کراراً در درس به کار می‌آیند را تحت نام **مرور** ذکر خواهیم کرد. این مطالب را می‌توان، بسته به سطح کلاس، مفروض گرفت یا به اختصار تدریس کرد یا به عنوان مطالعهٔ خارج معین نمود و یا آنکه مشروحاً درس داد. تلویحاً فرض است که دانشجو با قسمتهای مناسبی از فصل آشنایی آشناست (ر.ک. تذکر ۱، ص ذ). تقریباً همهٔ این دروس را می‌توان با حذف جمیع ***احکام ولمها ونتایج*** مربوطه‌شان کوتاه ساخت (ر.ک. ص خ).

نظریهٔ گروهها

مرور. آشنایی، حذف اکثر بخش ۸ (ر.ک. تذکر ۱، ص ذ).

درس *اصلی*. فصلهای یک و دو با حذف احتمالی بخشهای I. ۹، II. ۳، و نیمهٔ آخر II. ۷. همچنین می‌توان بخشهای II. ۱ و II. ۲ را حذف کرد یا دست‌کم تا بعد از قضایای زیلوف (بخش II. ۵) به تأخیر انداخت.

مدولها و ساختار حلقه‌ها

مرور. بخشهای III. ۱ و III. ۲ (تاقضیهٔ III. ۱۳.۲).

درس *اصلی*. بقیهٔ بخش III.۲؛ بخشهای ۱ تا ۵ از فصل چهار[1]؛ بخش VII.۱ (تاقضیهٔ VII.۱.۴)؛

---

۱. *اگر تأکید روی حلقه‌هاست، می‌توان بخش اعظم فصل چهار را حذف کرد. به طور مشخص، مطالب مورد نیاز عبارتند از بخش IV.۱، بخش IV.۲ (تا قضیهٔ IV.۲.۴)، تعریف IV.۲.۸، و بخش IV.۳ (تاتعریف IV.۳.۶).*

بخش VIII.1؛ بخشهای ۱ تا ۴ از فصل نه.

مباحث اضافی. بخشهای III.4، IV.6، IV.7، IX.5؛ بخش IV.5 در صورتی که قبلاً تدریس نشده است؛ بخش IX.6؛ مطالبی از فصل هشت.

میدانها و نظریهٔ گالوا

مرور. چند جمله‌ایها، مدولها، فضاهای برداری (بخشهای III.5، III.6، IV.1، IV.2). **گروههای** حلپذیر (بخشهای II.7 و II.8) در بخش V.9 به کار رفته‌اند.

درس اصلی[1]. بخشهای ۱ تا ۳ از فصل پنج با حذف ضمیمه‌ها؛ تعریف **V.4.1 و قضایای V.4.2** و V.4.12؛ بخش V.5 (تاقضیهٔ ۳.۵)؛ قضیهٔ V.6.2؛ بخش V.7 با حذف **حکم V.7.7 تا نتیجهٔ** V.7.9؛ قضیهٔ V.8.1؛ بخش V.9 (تا نتیجهٔ V.9.5)؛ بخش VI.1.

مباحث اضافی. بقیهٔ بخشهای V.5 و V.6 (دست کم تا تعریف V.6.10)؛ ضمیمه‌های بخش V.1 تا V.3؛ بقیهٔ بخشهای V.4، V.9، و V.7؛ بخش V.8؛ بخش VI.2.

جبر خطی

مرور. بخشهای ۳ تا ۶ فصل سه و بخش IV.1؛ قسمتهای انتخابی بخش IV.2 (فضاهای برداری با بعد متناهی).

درس اصلی. ساختار مدولهای تابی روی یک دامنهٔ ایده‌آل اصلی (بخش IV.6 با حذف مطالب مربوط به مدولهای آزاد)؛ بخشهای ۱ تا ۵ از فصل هفت با حذف ضمیمه‌ها و احتمالاً ***احکام***.

---

۱. خلاصهٔ درس مذکور در اینجا به نحوی طراحی شده است که حلپذیری معادلات چند جمله‌ای را می‌توان به سرعت بعد از قضیهٔ اساسی و میدانهای تجزیه‌گر عرضه کرد؛ این امر نیاز به استفاده از قضیهٔ V. 2.7 به جای تعریف V.1.7 به عنوان تعریف دارد. همانطور که تذکر پیش از قضیهٔ V.3.3 حاکی است، اگر فقط توسیعهای با بعد متناهی در نظرگرفته شود، بحث را می‌توان از آنچه هست کوتاهتر کرد.

جبر تعویضپذیر

مرور. بخشهای III.۱ و III.۲ (تاقضیهٔ III.۱۳.۲).

درس اصلی. بقیهٔ بخش III.۲؛ بخشهای III.۳ و III.۴؛ بخش IV.۱؛ بخش IV.۲ (تا نتیجهٔ IV.۲.۲)؛ بخش IV.۳ (تا حکم IV.۵.۳)؛بخشهای ۱ تا ۶ از فصل هشت با حذف احتمالی ***احکام.***

مباحث اضافی. بخش VIII.۷ (که خودنیاز به بخشهای V.۳ و VI.۱ دارد).

فهرست مطالب

آشنایی
پیشنیازها و مقدمات

در بخشهای ۱ تا ۶، برای راحتی خواننده، چند مطلب اساسی که فرض می‌کنیم کاملا" باآنهاآشناست (احتمالا" جزتمایز بین مجموعه‌ها و رده‌های حقیقی (بخش ۲)، توصیف حاصل ضرب دکارتی به وسیلهٔ خاصیت نگاشت عمومی (قضیهٔ ۲۰۵)، و قضیهٔ بازگشتی ۲۰۶) را خلاصه می‌کنیم. تعریف عدد اصلی (قسمت اول بخش ۸) مکرر به کار خواهد رفت. اصل انتخاب و معادلهایش (بخش ۷) و حساب اعداد اصلی (قسمت آخربخش ۸)رامی‌توان‌تازمانی که این اطلاعات عملا" به کار می‌روند به تعویق انداخت. بالاخره، فرض است که خواننده با میدانهای $\mathbf{Q}$، $\mathbf{R}$، و $\mathbf{C}$، یعنی اعداد گویا، حقیقی، و مختلط، آشنایی دارد.

۱ منطق

ما قراردادهای معمولی منطق را می‌پذیریم، و تنها جملاتی را در نظر می‌گیریم که ارزش راستی‌آنهاراست یا دروغ (نه هر دو) باشد (گزاره). هرگاه P و Q گزاره باشند، آنگاه گزارهٔ "P و Q" راست است اگر P و Q راست باشند، و در غیر این صورت دروغ می‌باشد. گزارهٔ "P یا Q" در جمیع حالات جزوقتی P و Q هر دو دروغند راست است. یک‌استلزام گزاره‌ای‌است به شکل "P ایجاب می‌کند Q را" یا "هرگاه P، آنگاه Q" (باعلامات، به‌صورت $P \Rightarrow Q$ نوشته می‌شود). یک استلزام دروغ است اگر P راست و Q دروغ باشد؛ و در جمیع حالات دیگر راست می‌باشد. بخصوص، *یک استلزام با مقدم دروغ همیشه راست است*. یک تعادل یا دو شرطی گزاره‌ای است به شکل "P ایجاب می‌کند Q را و Q ایجاب می‌کند P را". این معمولا" به صورت "P اگر و فقط اگر Q"

(با علامت $P \Leftrightarrow Q$ ، $P \Leftrightarrow Q$) خلاصه می‌شود. دو شرطی $P \Leftrightarrow Q$ فقط‌وقتی راست است که P و Q هر دو راست یا هر دو دروغ باشند؛ در غیر این صورت، دروغ خواهد بود. نقیض گزارهٔ P گزارهٔ "چنین نیست که P " است. این نقیض راست است اگر و فقط اگر P دروغ باشد.

۲ مجموعه‌ها و رده‌ها

روش ما در نظریهٔ مجموعه‌ها کاملا" غیرصوری است. معهذا، برای آنکه اعداد اصلی (بخش ۸) و رسته‌ها (بخش I ۷۰) به طرز شایسته‌ای تعریف شوند، لازم است دست‌کم مبادی اصل موضوعی سازی صوری نظریهٔ مجموعه‌ها معرفی گردند. درواقع، کل بحث را می‌توان، درصورت تمایل، کاملا" دقیق ساخت. ر.ک. ایزنبرگ[1] [۸] یا سوپه[2] [۱۰]. بحث اصل موضوعی نظریهٔ مجموعه‌ها برای احتراز از بعضی پارادکسها که در بحث کاملا" شهودی این مبحث تولید اشکال می‌کنند نیز سودمند است. یک پارادکس وقتی در یک دستگاه اصل موضوعی رخ می‌دهد که یک گزاره و نقیض قابل استنتاج از اصول موضوع باشند. این به نوبهٔ خود (با توجه به یک تمرین در منطق مقدماتی) ایجاب می‌کند که هر گزاره در دستگاه راست باشد، که مشکل بتوان آن را وضعیتی مطلوب دانست.

در نظریهٔ اصل موضوعی مجموعه‌ها به شکل گدل[3] ـ برنیز[4]، که ما تعقیب خواهیم کرد، مفاهیم اولیه (تعریف نشده) عبارتند از **رده**، **عضویت**، و **تساوی**. شهودا"، هر رده گردایه‌ای است مانند A از اشیاء (عنصرها) به طوری که، به ازای هر شیء x، بتوان مشخص کرد که x یک عضو (یا عنصر) A هست یا نه. برای " x یک عنصر A است" می‌نویسیم $x \in A$، و برای " x یک عنصر A نیست" می‌نویسیم $x \notin A$. اصول موضوع برحسب این مفاهیم اولیه و حساب محمولات مرتبهٔ اول (یعنی، زبان جملاتی که با استفاده از رابطهای **و**، **یا**، **چنین نیست که**، **ایجاب می‌کند**، و صورهای **وجود دارد** و **به ازای هر** ساخته می‌شوند) تنظیم می‌گردند. مثلا"، فرض است که تساوی خواص زیر را داراست: به ازای رده‌های دلخواه A, B, C، $A = A$؛ $A = B \Rightarrow B = A$؛ $A = B \Rightarrow A = C$؛ و $B = C$؛ $A = B \Rightarrow x \in B$ و $x \in A$. **اصل گسترش** حکم می‌کند که دو رده با عنصرهای

---

1. Eisenberg
2. Suppes
3. Gödel
4. Bernays

یکسان مساوی باشند (به‌طور صوری، $[x \in A \Leftrightarrow x \in B] \Rightarrow A = B$).

ردهٔ A یک **مجموعه** است اگر و فقط اگر رده‌ای مانند B باشد به طوری که $A \in B$. لذا، مجموعه نوع خاصی از رده است. هر رده که مجموعه نباشد یک **ردهٔ حقیقی** نامیده می‌شود. شهودا"، تمایز بین مجموعه‌ها و رده‌های حقیقی چندان واضح نیست. به بیان نادقیق، هر مجموعه یک ردهٔ "کوچک"، و هر ردهٔ حقیقی بی‌نهایت "بزرگ" است.

اصل تشکیل رده می‌گوید که، به ازای هر عبارت $P(y)$ در حساب محمولات مرتبهٔ اول شامل متغیر y، رده‌ای مانند A هست به طوری که $x \in A$ اگر و فقط اگر گزارهٔ $P(x)$ راست باشد. این A را با $\{x \mid P(x)\}$ نشان می‌دهیم، و آن را "ردهٔ تمام x هایی که $P(x)$" می‌خوانیم. گاهی یک رده صرفا با درج عناصرش در داخل دو ابرو توصیف می‌شود؛ مثلا"، $\{a,b,c\}$.

مثال[1]. ردهٔ $M = \{X \mid X \notin X\}$ یک مجموعه است و را در نظر می‌گیریم. عبارت $X \notin X$ نامعقول نیست، زیرا مجموعه‌های بسیاری در آن صدق می‌کنند (مثلا"، مجموعهٔ تمام کتابها کتاب نیست). M یک ردهٔ حقیقی است. زیرا هرگاه M یک مجموعه بود، $M \in M$ یا $M \notin M$. اما، طبق تعریف M، $M \in M$ ایجاب می‌کند که $M \notin M$، و $M \notin M$ ایجاب می‌کند که $M \in M$. لذا، در هر حال، فرض مجموعه بودن M به پارادکس غیرقابل دفاع $M \in M$ و $M \notin M$ ختم می‌شود.

حال چند مطلب آشنا (اجتماعها، اشتراکها، توابع، روابط، حاصل ضربهای دکارتی، و غیره) را مرور می‌کنیم. بحث ما غیرصوری است و ذکر اصول موضوع در اکثر جاها حذف شده است. اما فرض است که اصول موضوع کافی برای تضمین اینکه وقتی یکی از این ساختنها بر **مجموعه‌ها** اعمال شود، نتیجه نیز یک مجموعه است وجود دارند (مثلا"، اجتماع مجموعه‌ها یک مجموعه است؛ هر زیر ردهٔ یک مجموعه مجموعه است). طریقهٔ معمول در اثبات اینکه رده‌ای مجموعه است این است که نشان دهیم می‌توان آن را از یک مجموعه با رشته‌ای از این ساختنهای مجاز به دست آورد.

---

۱. *این برای اولین بار در ۱۹۰۲ (به شکلی نوعا" متفاوت) توسط برتران راسل* Bertrand Russell *به عنوان پارادکسی که لزوم اصل موضوعی سازی صوری نظریهٔ مجموعه‌ها را نشان داد بیان شده بود.*

ردهٔ A **زیر ردهٔ** ردهٔ B است (و می‌نویسیم $A \subset B$) مشروط بر اینکه

$$\text{به ازای هر } x,\ x \in A \Rightarrow x \in B. \qquad (۱)$$

بنابر اصول گسترش و خواص تساوی،

$$A = B \Leftrightarrow A \subset B \text{ و } B \subset A.$$

زیر ردهٔ A از ردهٔ B که خود مجموعه است یک **زیر مجموعهٔ** B نامیده می‌شود. اصول موضوعی وجود دارند که زیرمجموعه بودن یک زیر رده از یک مجموعه را تضمین می‌کنند.

مجموعهٔ تهی یا **مجموعهٔ پوچ** (که با $\varnothing$ نموده می‌شود) مجموعه‌ای است بدون عنصر (یعنی، به ازای هر x، $x \notin \varnothing$). چون عبارت $x \in \varnothing$ همیشه دروغ است، استلزام (۱) همواره وقتی $A = \varnothing$ راست می‌باشد. بنابراین، به ازای هر ردهٔ B، $\varnothing \subset B$. گوییم A یک زیر ردهٔ حقیقی B است اگر $A \subset B$ ولی $A \neq \varnothing$ و $A \neq B$.

اصل توان می‌گوید که، به ازای هر مجموعهٔ A، ردهٔ $P(A)$ مرکب از تمام زیرمجموعه‌های A خود یک مجموعه است. $P(A)$ **مجموعهٔ توان** A نام دارد؛ آن را با 2^A نیز نشان می‌دهند.

یک ***خانواده از مجموعه‌ها*** که به وسیلهٔ (ردهٔ ناتهی) I اندیسگذاری شده است گردایه‌ای است از **مجموعه‌های** A_i، یکی به ازای هر $i \in I$ (که با $\{A_i \mid i \in I\}$ نموده می‌شود). اگر چنین خانواده‌ای داشته باشیم، ***اجتماع*** و ***اشتراک*** آن به ترتیب مساوی رده‌های

$$\bigcup_{i \in I} A_i = \{x \mid \text{به ازای } i \in I \text{ ای }, x \in A_i\}$$

و

$$\bigcap_{i \in I} A_i = \{x \mid \text{به ازای هر } i \in I,\ x \in A_i\}$$

تعریف می‌شوند.

هرگاه I یک مجموعه باشد، آنگاه اصول موضوع مناسبی مجموعه بودن $\bigcup_{i \in I} A_i$ و $\bigcap_{i \in I} A_i$ را تضمین می‌کنند. اگر $I = \{1, 2, \ldots, n\}$، اغلب به جای $\bigcup_{i \in I} A_i$ می‌نویسند $A_1 \cup A_2 \cup \cdots \cup A_n$ و به همین ترتیب برای اشتراکها. اگر $A \cap B = \varnothing$، گویند A و B ***از هم جدا*** هستند.

اگر A و B رده باشند، **متمم نسبی** A در B زیر ردهٔ زیر از B است:

$$B - A = \{x \mid x \notin A \text{ و } x \in B\}.$$

هرگاه همهٔ رده‌های مورد بحث زیرمجموعه‌های مجموعهٔ ثابتی مانند U (به نام عالم سخن) باشند، آنگاه $U - A$ را با A' نموده و فقط می‌خوانند **متمم** A. بر خواننده است

که صحت احکام زیر را تحقیق نماید.

(۲)
$$A \cap (\bigcup_{i\in I} B_i) = \bigcup_{i\in I}(A \cap B_i)$$
$$A \cup (\bigcap_{i\in I} B_i) = \bigcap_{i\in I}(A \cup B_i).$$

(۳)
$$(\bigcup_{i\in I} A_i)' = \bigcap_{i\in I} A_i' \text{ و } (\bigcap_{i\in I} A_i)' = \bigcup_{i\in I} A_i'$$ (قوانین دمورگان[1]).

(۴)
$$A \cup B = B \iff A \subset B \iff A \cap B = A.$$

۳ تابعها

رده‌های A و B داده شده‌اند. **تابع** (یا **نگاشت**) f (نوشته می‌شود $f: A \to B$) به هر $a \in A$ دقیقاً یک عنصر $b \in B$ را مربوط می‌کند؛ b **مقدار تابع** در a یا **نقش** a نام دارد و معمولاً $f(a)$ نوشته می‌شود. A **دامنه** تابع است (گاهی نوشته می‌شود $\mathrm{Dom} f$) و B **برد** یا **هم‌دامنه** می‌باشد. گاهی شایسته است اثر تابع f بر عنصری از A با $a \mapsto f(a)$ نموده شود. دو تابع **مساوی**‌اند اگر یک دامنه و یک برد داشته و به ازای هر عنصر از دامنهٔ مشترکشان یک مقدار داشته باشند.

اگر $f: A \to B$ یک تابع بوده و $S \subset A$، تابع از S به B که به صورت زیر داده شده است:

$$a \mapsto f(a) \quad ، \quad a \in S \text{ به ازای}$$

تحدید f به S نام دارد و با $f|S: S \to B$ نموده می‌شود. اگر A یک رده باشد، **تابع همانی** بر A (که با $1_A: A \to A$ نموده می‌شود) تابعی است که با $a \mapsto a$ داده می‌شود. اگر $S \subset A$، تابع $1_A|S: S \to A$ **نگاشت‌شمول** S به‌توی A خوانده می‌شود.

فرض کنیم $f: A \to B$ و $g: B \to C$ تابع باشند. **ترکیب** f و g تابع $A \to C$ است که به صورت زیر داده می‌شود:

$$a \mapsto g(f(a)), \quad a \in A.$$

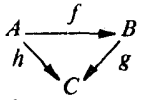
تابع مرکب با $g \circ f$ یا فقط gf نموده می‌شود. اگر $h: C \to D$ تابع سومی باشد، به‌آسانی

---

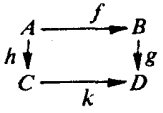
1. DeMorgan

تحقیق می‌شود که $h(gf) = (hg)f$. هرگاه $f: A \to B$ ، آنگاه $f \circ 1_A = f = 1_B \circ f: A \to B$.

نمودار



از توابع را **تعویضپذیر** گویند اگر $gf = h$. به‌همین‌ترتیب ، نمودار



تعویضپذیر است اگر $kh = gf$. ما مکرر با نمودارهای پیچیده‌تر مرکب از تعدادی مثلث و مربع مانند فوق سر و کار داریم . یک چنین نمودار را تعویضپذیر گویند اگر هر مثلث و مربع در آن تعویضپذیر باشد .

فرض کنیم $f: A \to B$ یک تابع باشد . اگر $S \subset A$ ، **نقش S تحت f** (که با $f(S)$ نموده می‌شود) رده‌ٔ

$$\{b \in B \mid b = f(a) \text{ ، ای } a \in S \text{ به ازای}\}$$

است . رده‌ٔ $f(A)$ **نقش f** نام دارد و گاهی با $\mathrm{Im} f$ نموده می‌شود . اگر $T \subset B$ ، **نقش معکوس T** تحت f (که با $f^{-1}(T)$ نموده می‌شود) رده‌ٔ

$$\{a \in A \mid f(a) \in T\}$$

می‌باشد . اگر T از یک عنصر تشکیل‌شده باشد ، یعنی $T = \{b\}$ ، به جای $f^{-1}(T)$ می‌نویسیم $f^{-1}(b)$. صحت احکام زیر را می‌توان به آسانی تحقیق کرد :

(۵) به ازای $S \subset A$ ، $f^{-1}(f(S)) \supset S$ ؛

(۶) به ازای $T \subset B$ ، $f(f^{-1}(T)) \subset T$ ؛

به ازای هر خانواده‌ٔ $\{T_i \mid i \in I\}$ از زیر مجموعه‌های B ،

(۷) $$f^{-1}(\bigcup_{i \in I} T_i) = \bigcup_{i \in I} f^{-1}(T_i);$$

(۸) $$f^{-1}(\bigcap_{i \in I} T_i) = \bigcap_{i \in I} f^{-1}(T_i).$$

تابع $f: A \to B$ را **انژکتیو** (یا **یک به یک**) گویند مشروط بر اینکه

به ازای هر $a, a' \in A$ ، $a \neq a' \Rightarrow f(a) \neq f(a')$ ؛

به بیان دیگر ، f انژکتیو است اگر و فقط اگر

به ازای هر $a,a' \in A$ ، $f(a) = f(a') \Rightarrow a = a'$.

تابع f **سورژکتیو** (یا **برو**) است مشروط بر اینکه $f(A) = B$ ؛ به عبارت دیگر ،

به ازای هر $b \in B$ ، $a \in A$ ای باشد به طوری که $b = f(a)$.

تابع f را **بیژکتیو** (یا **بیژکسیون** یا ***تناظر یک به یک***) گویند اگر هم انژکتیو و هم سورژکتیو باشد . از این تعاریف بی‌درنگ نتیجه می‌شود که ، به ازای هر ردهٔ A ، نگاشت همانی $1_A : A \to A$ بیژکتیو است . لازم است خواننده تحقیق کند که ، به ازای نگاشتهای $f : A \to B$ و $g : B \to C$ ،

(۹) gf انژکتیو است $\Rightarrow$ f و g انژکتیو ؛

(۱۰) gf سورژکتیو است $\Rightarrow$ f و g سورژکتیو ؛

(۱۱) f انژکتیو است $\Rightarrow$ gf انژکتیو ؛

(۱۲) g سورژکتیو است $\Rightarrow$ gf سورژکتیو .

قضیهٔ ۱.۳ . *فرض کنیم* $f : A \to B$ *یک تابع باشد ، با* A *ی ناتهی .*

(یک) f ***انژکتیو است اگر و فقط اگر نگاشتی مانند*** $g : B \to A$ ***باشد به طوری که*** $gf = 1_A$.

(دو) ***هرگاه*** A ***یک مجموعه باشد ، آنگاه*** f ***سورژکتیو است اگر و فقط اگر نگاشتی مانند*** $h : B \to A$ ***باشد به طوری که*** $fh = 1_B$.

برهان . چون هر نگاشت همانی بیژکتیو است ، (۱۱) و (۱۲) استلزامهای ($\Leftarrow$) در (یک) و (دو) را ثابت می‌کنند . به عکس ، هرگاه f انژکتیو باشد ، آنگاه به ازای هر $b \in f(A)$ ، $a \in A$ ای منحصر به فرد وجود دارد که $f(a) = b$. $a_0 \in A$ ثابت اختیار کرده و تحقیق می‌کنیم نگاشت $g : B \to A$ تعریف شده با

$$g(b) = \begin{cases} a \ . \ f(a) = b & \text{اگر } b \in f(A) \text{ و} \\ a_0 & \text{اگر } b \notin f(A) \ , \end{cases}$$

چنان است که $gf = 1_A$. برای عکس (دو) فرض می‌کنیم f سورژکتیو باشد . پس به ازای هر $b \in B$ ، $f^{-1}(b) \subset A$ ، یک مجموعهٔ ناتهی است . به ازای هر $b \in B$ ، $a_b \in f^{-1}(b)$ را اختیار می‌کنیم (**تذکر .** این نیاز به اصل انتخاب دارد ؛ ر.ک . بخش ۷) . تحقیق کنید که نگاشت $h : B \to A$ تعریف شده با $h(b) = a_b$ چنان است که $fh = 1_B$.

نگاشت g در قضیهٔ ۱.۳ یک **معکوس چپ** f ، و h یک **معکوس راست** f نام دارد. هرگاه نگاشت $f: A \to B$ هم معکوس چپ g و هم معکوس راست h داشته باشد، آنگاه

$$g = g1_B = g(fh) = (gf)h = 1_A h = h$$

و نگاشت $g = h$ یک **معکوس دوطرفهٔ** f نامیده می‌شود. این استدلال همچنین نشان می‌دهد که معکوس دوطرفهٔ یک نگاشت (در صورت وجود) منحصر به فرد است. طبق قضیهٔ ۱.۳ ، هرگاه A یک مجموعه بوده و $f: A \to B$ یک تابع باشد، آنگاه

f دارای معکوس دوطرفه باشد $\Leftrightarrow$ f بیژکتیو است [1] (۱۳)

معکوس دوطرفهٔ منحصر به فرد بیژکسیون f با f^{-1} نموده می‌شود؛ واضح است که f یک معکوس دوطرفهٔ f^{-1} است؛ در نتیجه، f^{-1} نیز یک بیژکسیون می‌باشد.

۴ رابطه‌ها و افرازها

اصل تشکیل جفت می‌گوید که، به ازای هر دو مجموعهٔ [عنصرهای] a,b ، یک مجموعه مانند $P = \{a,b\}$ وجود دارد به طوری که $x \in P$ اگر و فقط اگر $x = a$ یا $x = b$ ؛ هرگاه $a = b$ ، آنگاه P یکانی $\{a\}$ است. **جفت مرتب** (a,b) مساوی مجموعهٔ $\{\{a\},\{a,b\}\}$ تعریف می‌شود؛ **مولفهٔ اول** آن a و **مولفهٔ دوم** آن b است. به آسانی تحقیق می‌شود که $(a,b) = (a',b')$ اگر و فقط اگر $a = a'$ و $b = b'$. **حاصل‌ضرب دکارتی** رده‌های A و B رده‌ٔ

$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

است. توجه کنید که $A \times \varnothing = \varnothing = \varnothing \times B$.

هر زیر رده‌ٔ R از $A \times B$ یک **رابطه** بر $A \times B$ نامیده می‌شود. مثلاً، اگر $f: A \to B$ یک تابع باشد، **نمودار** f رابطهٔ $R = \{(a,f(a)) \mid a \in A\}$ است. چون f یک تابع است، R خاصیت ویژهٔ زیر را دارد:

هر عنصر A مولفهٔ اول یک و فقط یک جفت مرتب در R است. (۱۴)

به عکس، هر رابطهٔ R بر $A \times B$ که در (۱۴) صدق کند تابع منحصر به فردی مانند $f: A \to B$ را معین می‌کند که نمودارش R است (کافی است تعریف کنیم $f(a) = b$ ، که

---

۱. *گزارهٔ (۱۳) در واقع حتی وقتی A یک رده‌ٔ حقیقی باشد نیز راست است*؛ ر.ک. ایزنبرگ [۸؛ ص ۱۴۶] .

در آن (a,b) جفت مرتب منحصر به فرد در R با مولفهٔ اول a است). به این دلیل معمولاً در ارائهٔ اصل موضوعی صوری نظریهٔ مجموعه‌ها یک تابع را با نمودارش یکی می‌گیرند؛ یعنی، یک تابع را رابطه‌ای **تعریف** می‌کنند که در (۱۴) صدق کند. این کار، مثلاً، برای اثبات مجموعه بودن نقش یک مجموعه تحت یک تابع از اصول موضوع لازم است.

مزیت دیگر این کار آن است که به ما اجازهٔ تعریف توابع با دامنهٔ تهی را می‌دهد. زیرا چون $\varnothing \times B = \varnothing$ زیر مجموعهٔ منحصر به فرد $\varnothing \times B$ است و به طور خالی در (۱۴) صدق می‌کند، تابعی منحصر به فرد مانند $\varnothing \to B$ وجود دارد. همچنین، از (۱۴) واضح است که یک تابع با برد تهی می‌تواند وجود داشته باشد فقط اگر دامنه نیز تهی باشد. هر جا مناسب بود، یک تابع را رابطه‌ای تصور خواهیم کرد که در (۱۴) صدق می‌کند.

رابطهٔ R بر $A \times A$ یک **رابطهٔ هم‌ارزی** بر A است مشروط بر اینکه

منعکس: به ازای هر $a \in A$، $(a,a) \in R$؛ (۱۵)

متقارن: $(a,b) \in R \Rightarrow (b,a) \in R$؛ (۱۶)

متعدی: $(a,b) \in R$ و $(b,c) \in R \Rightarrow (a,c) \in R$. (۱۷)

اگر R یک رابطهٔ هم‌ارزی بر A بوده و $(a,b) \in R$، گوییم a **هم‌ارز** b تحت R است و می‌نویسیم $a \sim b$ یا aRb؛ با این نمادگذاری، (۱۵) تا (۱۷) خواهند شد:

$$a \sim a; \tag{۱۵′}$$

$$a \sim b \Rightarrow b \sim a; \tag{۱۶′}$$

$$a \sim b \text{ و } b \sim c \Rightarrow a \sim c. \tag{۱۷′}$$

فرض کنیم R ($\sim$) یک رابطهٔ هم‌ارزی بر A باشد. اگر $a \in A$، **ردهٔ هم‌ارزی** a (که با $\bar{a}$ نموده می‌شود) ردهٔ تمام عناصری از A است که هم‌ارز a اند؛ یعنی، $\bar{a} = \{b \in A \mid b \sim a\}$. ردهٔ تمام رده‌های هم‌ارزی در A با A/R نموده و **ردهٔ خارج قسمتی** A بر R نامیده می‌شود. چون R منعکس است، به ازای هر $a \in A$، $a \in \bar{a}$؛ از اینرو،

به ازای هر $a \in A$، $\bar{a} \neq \varnothing$؛ (۱۸)

و اگر A یک مجموعه باشد،

$$\bigcup_{a \in A} \bar{a} = A = \bigcup_{\bar{a} \in A/R} \bar{a}. \tag{۱۹}$$

همچنین ، ملاحظه می‌کنیم که

$$\bar{a} = \bar{b} \iff a \sim b; \tag{۲۰}$$

زیرا هرگاه $\bar{a} = \bar{b}$ ، آنگاه $a \in \bar{a} \Rightarrow a \in \bar{b} \Rightarrow a \sim b$. به عکس، هرگاه $a \sim b$ و $c \in \bar{a}$ ، آنگاه $c \sim a \Rightarrow c \sim b \Rightarrow c \in \bar{b}$ و $a \sim b$. لذا، $\bar{a} \subset \bar{b}$ ؛ استدلالی متقارن نشان می‌دهد که $\bar{b} \subset \bar{a}$ ؛ و لذا، $\bar{a} = \bar{b}$. حال ثابت می‌کنیم

$$\text{به ازای } a,b \in A \text{ ، } \bar{a} = \bar{b} \text{ یا } \bar{a} \cap \bar{b} = \varnothing \text{ .} \tag{۲۱}$$

هرگاه $\bar{a} \cap \bar{b} \neq \varnothing$ ، آنگاه عنصری مانند $c \in \bar{a} \cap \bar{b}$ موجود است . از اینرو، $c \sim a$ و $c \sim b$. با استفاده‌از تقارن ، تعدی ، و (۲۰) داریم $a \sim c \Rightarrow a \sim b \Rightarrow \bar{a} = \bar{b}$ و $c \sim b$.

فرض کنیم A یک رده‌ٔ ناتهی بوده و $\{A_i \mid i \in I\}$ خانواده‌ای از زیرمجموعه‌های A باشد به طوری که

$$\text{به ازای هر } i \in I \text{ ، } A_i \neq \varnothing \text{ ؛}$$

$$\bigcup_{i \in I} A_i = A;$$

$$\text{به ازای هر } i \neq j \in I \text{ ، } A_i \cap A_j = \varnothing \text{ ؛}$$

در این صورت ، $\{A_i \mid i \in I\}$ یک ***افراز*** A نامیده می‌شود .

قضیهٔ ۱۰۴ . *هرگاه* A *یک مجموعهٔ ناتهی باشد ، آنگاه ارتباط* $R \mapsto A/R$ *یک بیژکسیون از مجموعهٔ* $E(A)$ *همهٔ روابط هم‌ارزی بر* A *به روی مجموعهٔ* $Q(A)$ *تمام افرازهای* A *تعریف می‌کند .*

طرح برهان . هرگاه R یک رابطهٔ هم‌ارزی بر A باشد ، آنگاه ، بنابر (۱۸) ، (۱۹) ، و (۲۱) ، مجموعهٔ رده‌های هم‌ارزی A/R یک افراز است ؛ درنتیجه ، $R \mapsto A/R$ یک تابع مانند $f : E(A) \to Q(A)$ تعریف می‌کند . تابع $g : Q(A) \to E(A)$ را به صورت زیر تعریف می‌کنیم . اگر $S = \{A_i \mid i \in I\}$ افرازی‌از A باشد ، رابطهٔ هم‌ارزی $g(S)$ بر A را به صورت زیر می‌گیریم :

$$\text{به ازای } i \in I \text{ ی (منحصر به فرد) ، } a \in A_i \text{ و } b \in A_i \iff a \sim b \tag{۲۲}$$

تحقیق کنید که $g(S)$ در واقع یک رابطهٔ هم‌ارزی است به‌طوری که به ازای $a \in A_i$ ، $\bar{a} = A_i$. برهان با تحقیق اینکه $fg = 1_{Q(A)}$ و $gf = 1_{E(A)}$ کامل می‌شود . در این صورت،

بنابر (۱۳)، f بیژکتیو است.

۵ حاصل ضربها

تذکر. در این بخش فقط *با مجموعه‌ها* سروکار داریم. هیچ ردهٔ حقیقی در کار نخواهد آمد.

حاصل ضرب دکارتی $A_1 \times A_2$ دو مجموعه را در نظر می‌گیریم. هر عنصر $A_1 \times A_2$ جفتی است مانند (a_1,a_2) با $a_i \in A_i$ و $i = 1,2$. لذا، جفت (a_1,a_2) تابع $f:\{1,2\} \to A_1 \cup A_2$ با تعریف $f(1) = a_1$ و $f(2) = a_2$ را معین می‌کند. به عکس، هر تابع $f:\{1,2\} \to A_1 \cup A_2$ با خاصیت $f(1) \in A_1$ و $f(2) \in A_2$ عنصر $(a_1,a_2) = (f(1),f(2))$ از $A_1 \times A_2$ را معین می‌کند. لذا، به آسانی می‌بینیم که تناظر یک به یکی بین مجموعهٔ تمام توابع از این نوع و مجموعهٔ $A_1 \times A_2$ وجود دارد. این ما را به تعمیم مفهوم حاصل ضرب دکارتی به صورت زیر هدایت می‌کند.

تعریف ۱۰۵. فرض کنیم $\{A_i \mid i \in I\}$ خانواده‌ای از مجموعه‌ها باشد که به‌وسیلهٔ مجموعهٔ (ناتهی) I اندیسگذاری شده‌اند. ***حاصل ضرب (دکارتی)*** مجموعه‌های A_i مجموعهٔ تمام توابع $f: I \to \bigcup_{i \in I} A_i$ است به طوری که به ازای هر $i \in I$، $f(i) \in A_i$. این حاصل‌ضرب با $\prod_{i \in I} A_i$ نموده می‌شود.

هرگاه $I = \{1,2,\ldots,n\}$، حاصل‌ضرب $\prod_{i \in I} A_i$ اغلب با $A_1 \times A_2 \times \cdots \times A_n$ نموده شده و با مجموعهٔ تمام n تاییهای مرتب $(a_1,a_2,\ldots,a_n)$، که به ازای $i = 1,2,\ldots,n$، $a_i \in A_i$، یکی گرفته می‌شود، درست مثل حالت مذکور در بالا، که در آن $I = \{1,2\}$. اغلب وقتی I نامتناهی است نماد مشابهی به کار می‌رود. گاهی تابع $f \in \prod_{i \in I} A_i$ را با $(a_i)_{i \in I}$ یا فقط (a_i) نشان می‌دهیم، که در آن به ازای هر $i \in I$، $f(i) = a_i \in A_i$.

هرگاه $A_i = \varnothing$ ای، آنگاه $\prod_{i \in I} A_i = \varnothing$، زیرا تابعی مانند $f: I \to \bigcup A_i$ نمی‌تواند موجود باشد که $f(i) \in A_i$.

هرگاه $\{A_i \mid i \in I\}$ و $\{B_i \mid i \in I\}$ خانواده‌هایی از مجموعه‌ها باشند به‌طوری که به‌ازای هر $i \in I$ ، $B_i \subset A_i$ ، آنگاه هرتابع $I \to \bigcup_{i \in I} B_i$ را می‌توان تابعی مانند $I \to \bigcup_{i \in I} A_i$ منظور کرد. لذا، $\prod_{i \in I} B_i$ را زیرمجموعه‌ای از $\prod_{i \in I} A_i$ در نظر می‌گیریم.

فرض کنیم $\prod_{i \in I} A_i$ یک حاصل ضرب دکارتی باشد. به ازای هر $k \in I$ ، نگاشت $\pi_k : \prod_{i \in I} A_i \to A_k$ را با $f \mapsto f(k)$ تعریف می‌کنیم، یا با نماد دیگر، $\{a_i\} \mapsto a_k$. π_k **تصویر (کانونی)** حاصل‌ضرب روی مؤلفهٔ (یا عامل) k ام نام دارد. هرگاه هر A ناتهی باشد، آنگاه هر π_k سورژکتیو است (ر.ک. تمرین ۶.۷).

حاصل‌ضرب $\prod_{i \in I} A_i$ وتصاویرش درست همان ابزاری هستند که در اثبات قضیهٔ زیر لازمند.

قضیهٔ ۲.۵ . *فرض کنیم $\{A_i \mid i \in I\}$ خانواده‌ای از مجموعه‌ها باشد که به‌وسیلهٔ I اندیسگذاری شده‌اند. در این صورت، مجموعهٔ D همراه با خانوادهٔ $\{\pi_i : D \to A_i \mid i \in I\}$ از نگاشتها با خاصیت زیر وجود دارند: به‌ازای هر مجموعهٔ C و خانوادهٔ $\{\varphi_i : C \to A_i \mid i \in I\}$ از نگاشتها، نگاشت منحصر به فردی مانند $\varphi : C \to D$ هست به‌طوری که به‌ازای هر $i \in I$ ، $\pi_i \varphi = \varphi_i$. به علاوه، D با تقریب بیژکسیون منحصر به فرد است.*

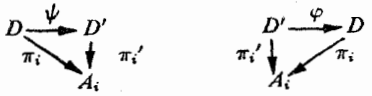
جملهٔ آخر به این معنی است که هرگاه D' یک مجموعه و $\{\pi_i' : D' \to A_i \mid i \in I\}$ خانواده‌ای از نگاشتها با همان خاصیت D و $\{\pi_i\}$ باشند، آنگاه یک بیژکسیون مانند $D \to D'$ وجود دارد.

برهان ۲.۵ (وجود) . فرض کنیم $D = \prod_{i \in I} A_i$ و نگاشتهای π_i تصویرها روی مؤلفه‌های iام باشند. به‌فرض‌داده‌شدن C ونگاشتهای φ_i ، $\varphi : C \to \prod_{i \in I} A_i$ را با $c \mapsto f_c$ تعریف می‌کنیم، که در آن $f_c(i) = \varphi_i(c) \in A_i$. فورا" نتیجه می‌شود که به ازای هر $i \in I$ ، $\pi_i \varphi = \varphi_i$. برای آنکه نشان دهیم φ منحصر به فرد است، فرض می‌کنیم $\varphi' : C \to \prod_{i \in I} A_i$

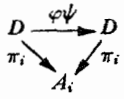
نگاشتی دیگر باشد به طوری که به ازای هر $i \in I$ ، $\pi_i\varphi' = \varphi_i$ ، و ثابت می‌کنیم $\varphi = \varphi'$. برای این‌کار باید نشان دهیم که به ازای هر $c \in C$ ، $\varphi(c)$ و $\varphi'(c)$ عنصرهای یکسانی از $\coprod_{i\in I} A_i$ اند ؛ یعنی ، $\varphi(c)$ و $\varphi'(c)$ به‌عنوان توابعی بر I یکی هستند : به ازای هر $i \in I$ ، $(\varphi(c))(i) = (\varphi'(c))(i)$. امـــا ، طبق فرض و تعریف π_i ، به ازای هر $i \in I$ داریم

$$(\varphi'(c))(i) = \pi_i\varphi'(c) = \varphi_i(c) = f_c(i) = (\varphi(c))(i).$$

(یکتایی) . فرض کنیم D' (با نگاشتهای $\pi_i' : D' \to A_i$) همان خاصیت $D = \coprod_{i\in I} A_i$ را داشته بـاشد . اگر این خاصیت (از D) را بر خانواده‌ٔ $\{\pi_i' : D' \to A_i\}$ از نگاشتها ، و نیز ایـن خـاصیت (از D') را بـر خانواده‌ٔ $\{\pi_i : D \to A_i\}$ اعمال کنیم ، نگاشتهای (منحصر به فرد) $\varphi : D' \to D$ و $\psi : D \to D'$ به دست می‌آوریـم به‌طوری که نمودارهای



به ازای هر $i \in I$ تعویضپذیرند . از تلفیق این نمودارها ، نمودار تعویضپذیر



به ازای هر $i \in I$ نتیجه می‌شود . لذا ، نگاشت $\varphi\psi : D \to D$ چنان است که به ازای هر $i \in I$ ، $\pi_i(\varphi\psi) = \pi_i$. اما ، طبـق برهان فوق ، نگاشت منحصر به‌فردی با این خاصیت وجود دارد . چون نگاشت $1_D : D \to D$ نیز طوری است که به ازای هر $i \in I$ ، $\pi_i 1_D = \pi_i$ ، باید طبق یکتایی داشته باشیم $\varphi\psi = 1_D$. استدلالی مشابه نشان می‌دهد که $\psi\varphi = 1_{D'}$.

لذا ، φ طبق (۱۳) یک بیژکسیون است و $D = \coprod_{i\in I} A_i$ با تقریب بیژکسیون به‌طور منحصر به فرد معین می‌شود .

توجه کنید که در صورت قضیـهٔ ۲.۵ ذکـری از عنصر نشده است ، و فقط مستلزم مجموعه‌ها و نگاشتهاست . این قضیه ، درواقع ، می‌گوید که حاصل ضرب $\coprod_{i\in I} A_i$ به وسیلهٔ

خاصیت نگاشت عمومی توصیف می‌شود. این مفهوم را زمان پرداختن به رسته‌ها و تابعگرها دقیقتر خواهیم ساخت.

۶ اعداد صحیح

ما قصد پرداختن به اعداد صحیح به شکل اصل موضوعی نداریم. در عوض، فرض می‌کنیم خواننده با مجموعهٔ اعداد صحیح $\mathbf{Z}$، مجموعهٔ اعداد صحیح نامنفی $\mathbf{N} = \{0,1,2,\ldots\}$ (یا اعداد طبیعی)، مجموعهٔ اعداد صحیح مثبت $\mathbf{N}^* = \{1,2,\ldots\}$، و خواص ابتدایی جمع، ضرب، و ترتیب کاملا" آشنا باشد. بالاخص، به‌ازای هر $a,b,c \in \mathbf{Z}$،

$(a+b)+c = a+(b+c)$ و $(ab)c = a(bc)$ (قوانین شرکتپذیری): (۲۳)

$a+b = b+a$ و $ab = ba$ (قوانین تعویضپذیری)؛ (۲۴)

$a(b+c) = ab+ac$ و $(a+b)c = ac+bc$ (قوانین پخشپذیری)؛ (۲۵)

$a+0 = a$ و $a1 = a$ (عنصرهای همانی)؛ (۲۶)

به‌ازای هر $a \in \mathbf{Z}$، عددی مانند $-a \in \mathbf{Z}$ هست به طوری‌که خواهیم داشت $a+(-a) = 0$ (معکوس جمعی)؛ (۲۷)

به جای $a+(-b)$ می‌نویسیم $a-b$.

$a = 0$ یا $b = 0 \Leftrightarrow ab = 0$؛ (۲۸)

به ازای هر $c \in \mathbf{Z}$، $a < b \Rightarrow a+c < b+c$؛ (۲۹)

به ازای هر $d \in \mathbf{N}^*$، $a < b \Rightarrow ad < bd$. (۳۰)

ما $a < b$ و $b > a$ را به جای هم می‌نویسیم و نیز، اگر $a < b$ یا $a = b$، خواهیم نوشت $a \leq b$. قدر مطلق $a \in \mathbf{Z}$، یعنی $|a|$، مساوی a اگر $a \geq 0$ و مساوی $-a$ اگر $a < 0$ تعریف می‌شود. بالاخره، اصل زیر را به عنوان یک اصل موضوع اساسی می‌پذیریم.

قانون خوش ترتیبی. هر زیر مجموعهٔ ناتهی S از $\mathbf{N}$ شامل کوچکترین عنصر است (یعنی، عنصری مانند $b \in S$ هست به‌طوری‌که به‌ازای هر $c \in S$، $b \leq c$).

بویژه، 0 کوچکترین عنصر $\mathbf{N}$ می‌باشد.

علاوه بر مطالب فوق، به چند نکته از نظریهٔ مقدماتی اعداد نیاز داریم، که برخی از آنها را در اینجا به اختصار مرور می‌کنیم.

قضیهٔ ۱.۶ (اصل استقرای ریاضی). *هرگاه S زیرمجموعه‌ای از مجموعهٔ اعداد طبیعی $\mathbf{N}$ باشد به طوری که $0 \in S$ و*

(یک) به ازای هر $n \in \mathbf{N}$، $n \in S \Rightarrow n+1 \in S$

یا

(دو) به‌ازای هر $n \in \mathbf{N}$، $n \in S \Rightarrow$ به‌ازای هر m که $0 \leq m < n$، $m \in S$، آنگاه $S = \mathbf{N}$.

برهان. اگر $\mathbf{N} - S \neq \varnothing$، $n \neq 0$ را کوچکترین عنصر آن می‌گیریم. پس به‌ازای هر $m < n$، باید داشته باشیم $m \notin \mathbf{N} - S$؛ و در نتیجه، $m \in S$. لذا، (یک) یا (دو) $n \in S$ را ایجاب می‌کند، که یک تناقض است. بنابراین، $\mathbf{N} - S = \varnothing$ و $S = \mathbf{N}$.

تبصره. قضیهٔ ۱.۶ همچنین وقتی $\mathbf{N}$ و 0 با $M_c = \{x \in \mathbf{Z} \mid x \geq c\}$ و c، به‌ازای هر $c \in \mathbf{Z}$، عوض شوند نیز برقرار است.

برای اطمینان از اعتبار تعاریف و برهانهای بازگشتی یا استقرایی درآینده (مثلاً"، قضایای ۸.۸ و III، ۷.۳ در زیر)، به یک نتیجهٔ تکنیکی نیاز داریم:

قضیهٔ ۲.۶ (قضیهٔ بازگشتی). *هرگاه S یک مجموعه بوده، $a \in S$، و به ازای هر $n \in \mathbf{N}$، $f_n : S \to S$ یک تابع باشد، آنگاه تابع منحصر به فردی مانند $\varphi : \mathbf{N} \to S$ هست به‌طوری که $\varphi(0) = a$ و به‌ازای هر $n \in \mathbf{N}$، $\varphi(n+1) = f_n(\varphi(n))$.*

طرح برهان. رابطهٔ R بر $\mathbf{N} \times S$ را طوری می‌سازیم که نمودار تابعی مانند $\varphi : \mathbf{N} \to S$ با خواص مطلوب باشد. فرض کنیم $\mathcal{G}$ مجموعهٔ تمام زیرمجموعه‌های Y از $\mathbf{N} \times S$ باشد به طوری‌که

به‌ازای هر $n \in \mathbf{N}$، $(0,a) \in Y$ و $(n,x) \in Y \Rightarrow (n+1, f_n(x)) \in Y$.

در این صورت $\mathcal{G} \neq \varnothing$، زیرا $\mathbf{N} \times S \in \mathcal{G}$؛ پس $R \in \mathcal{G}$. فرض کنیم $R = \bigcap_{Y \in \mathcal{G}} Y$ قرار می‌دهیم

زیر مجموعه‌ای از $\mathbf{N}$ مرکب از تمام $n \in \mathbf{N}$ هایی باشد که به ازای آنها $x_n \in S$ ی منحصر به فرد موجود باشد به طوری که $(n, x_n) \in R$. به استقرا ثابت می‌کنیم که $M = \mathbf{N}$. هرگاه

$0 \notin M$ ، آنگاه $(0,b) \in R$ ای با $b \neq a$ وجود دارد و مجموعهٔ $R - \{(0,b)\} \subset \mathbf{N} \times S$ در $\mathcal{G}$ می‌باشد. درنتیجه، $R = \bigcap_{Y \in \mathcal{G}} Y \subset R - \{(0,b)\}$ ، که تناقض است. لذا، $0 \in \mathbf{M}$. به استقرا، فرض کنیم $n \in M$ (یعنی، به‌ازای یک $x_n \in S$ منحصر به فرد، $(n,x_n) \in R$) . در این صورت، نیز $(n+1,f_n(x_n)) \in R$. هرگاه $(n+1,c) \in R$ و $c \neq f_n(x_n)$ ، آنگاه $R - \{(n+1,c)\} \in \mathcal{G}$ (تحقیق کنید!) ، که مثل بالا به تناقض ختم می‌شود. بنابراین، $x_{n+1} = f_n(x_n)$ عنصر منحصر به فردی از مجموعهٔ S است که $(n+1,x_{n+1}) \in R$. بنابراین به استقرا (قضیهٔ ۱.۶) ، $\mathbf{N} = M$ ؛ لذا، ارتباط $n \mapsto x_n$ تابعی مانند $\varphi : \mathbf{N} \to S$ با نمودار R را تعریف می‌کند. چون $(0,a) \in R$ ، باید داشته باشیم $\varphi(0) = a$. به‌ازای هر $n \in \mathbf{N}$ ، $(n,x_n) = (n,\varphi(n)) \in R$ ؛ و در نتیجه، $(n+1,f_n(\varphi(n))) \in R$ ، زیرا $R \in \mathcal{G}$. اما $(n+1,x_{n+1}) \in R$ و یکتایی x_{n+1} ایجاب می‌کند که $\varphi(n+1) = x_{n+1} = f_n(\varphi(n))$.

هرگاه A مجموعه‌ای ناتهی باشد، آنگاه یک **دنباله** در A تابعی است مانند $\mathbf{N} \to A$. یک دنباله معمولاً با $\{a_0,a_1,\ldots\}$ یا $\{a_i\}_{i \in N}$ یا $\{a_i\}$ ، که $a_i \in A$ نقش $i \in \mathbf{N}$ است، نموده می‌شود. به همین نحو، هر تابع $\mathbf{N}^* \to A$ نیز یک دنباله نامیده و با $\{a_1,a_2,\ldots\}$ یا $\{a_i\}_{i \in \mathbf{N}^*}$ یا $\{a_i\}$ نموده می‌شود؛ این در متن ابهامی تولید نخواهد کرد.

قضیهٔ ۳.۶ (الگوریتم تقسیم). *هرگاه $a,b, \in \mathbf{Z}$ و $a \neq 0$ ، آنگاه اعداد صحیح منحصر به فردی مانند q و r وجود دارند به طوری که $b = aq + r$ و $0 \leq r < |a|$.*

طرح برهان. نشان دهید که مجموعهٔ $S = \{b - ax \mid x \in \mathbf{Z}, b - ax \geq 0\}$ یک زیرمجموعهٔ ناتهی از $\mathbf{N}$ است؛ ولذا، دارای کوچکترین عنصر مانند $r = b - aq$ (به‌ازای $q \in \mathbf{Z}$ ای) می‌باشد. بنابراین، $b = aq + r$. با استفاده از کوچکترین عنصر بودن r در S ، برقراری $0 \leq r < |a|$ و یکتایی r و q را نشان دهید.

گوییم عدد صحیح $a \neq 0$ عدد صحیح b را **عاد می‌کند** (می‌نویسیم $a \mid b$) اگر عدد صحیحی مانند k باشد به‌طوری‌که $ak = b$. اگر a ، b را عاد نکند، می‌نویسیم $a \nmid b$.

تعریف ۴۰۶. گوییم عدد صحیح و مثبت c **بزرگترین مقسوم‌علیه مشترک** اعداد صحیح $a_1, a_2, \ldots, a_n$ است اگر

(۱) به‌ازای $1 \le i \le n$ ، $c \mid a_i$ ؛

(۲) $d \in \mathbf{Z} \Rightarrow d \mid c$ و به‌ازای $1 \le i \le n$ ، $d \mid a_i$

c را با $(a_1, a_2, \ldots, a_n)$ نشان می‌دهند.

قضیهٔ ۵۰۶. *هرگاه* $a_1, a_2, \ldots, a_n$ *اعدادی صحیح بوده و همه* 0 *نباشند ، آنگاه* $(a_1, a_2, \ldots, a_n)$ *وجود دارد. به علاوه ، اعداد صحیحی مانند* $k_1, k_2, \ldots, k_n$ *وجود دارند به‌طوری‌که*

$$(a_1, a_2, \ldots, a_n) = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n.$$

طرح برهان. با استفاده از الگوریتم تقسیم ، نشان دهید که کوچکترین عنصر مثبت مجموعهٔ ناتهی

$$S = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \mid x_i \in \mathbf{Z}, \sum_i x_i a_i > 0\}$$

بزرگترین مقسوم‌علیه مشترک $a_1, \ldots, a_n$ است. برای مشاهدهٔ جزئیات ، ر.ک شوکلی[1] [۵۱، ص ۱۰].

اعداد صحیح $a_1, a_2, \ldots, a_n$ را **نسبت به هم اول** گویند اگر $(a_1, a_2, \ldots, a_n) = 1$. عدد صحیح و مثبت $p > 1$ را **اول** گویند اگر تنها مقسوم‌علیه‌های آن ± 1 و $\pm p$ باشند. لذا ، اگر p اول بوده و $a \in \mathbf{Z}$ ، $(a, p) = p$ (اگر $p \mid a$) یا $(a, p) = 1$ (اگر $p \nmid a$).

قضیهٔ ۶۰۶. *هرگاه* a *و* b *اعدادی صحیح و نسبت به هم اول باشند و* $a \mid bc$ *، آنگاه* $a \mid c$. *هرگاه* p *اول بوده و* $p \mid a_1 a_2 \cdots a_n$ *، آنگاه به‌ازای* i *ی* ، $p \mid a_i$.

طرح برهان. طبق قضیهٔ ۵۰۶ ، $1 = ra + sb$ ، که از آنجا $c = rac + sbc$. بنابراین ، $a \mid c$. حال حکم دوم را می‌توان به استقرا بر n نتیجه گرفت.

---

1. Shockley

قضیهٔ ۷.۶ (قضیهٔ اساسی حساب). *هر عدد صحیح مثبت $n > 1$ را می‌توان به طور منحصر به فرد به شکل $n = p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$ نوشت، که در آن $p_1 < p_2 < \cdots < p_k$ اعدادی اول بوده و به‌ازای هر i، $t_i > 0$.*

اثبات، که به استقرا است، را می‌توان در شوکلی [۵۱، ص ۱۷] یافت.

فرض کنیم $m > 0$ عدد صحیح ثابتی باشد. هرگاه $a,b \in \mathbf{Z}$ و $m \mid (a-b)$، آنگاه گویند a همنهشت b به پیمانهٔ m است. این را با $a \equiv b \pmod m$ نشان می‌دهند.

قضیهٔ ۸.۶. فرض کنیم $m > 0$ عددی صحیح بوده و $a,b,c,d \in \mathbf{Z}$.

(یک) *همنهشتی به پیمانهٔ m یک رابطهٔ هم‌ارزی بر مجموعهٔ اعداد صحیح $\mathbf{Z}$ است، که دقیقاً m ردهٔ هم‌ارزی دارد.*

(دو) *هرگاه $a \equiv b \pmod m$ و $c \equiv d \pmod m$، آنگاه $a+c \equiv b+d \pmod m$ و $ac \equiv bd \pmod m$.*

(سه) *هرگاه $ab \equiv ac \pmod m$ و a و m نسبت به هم اول باشند، آنگاه $b \equiv c \pmod m$.*

برهان (یک). این امر که همنهشتی به پیمانهٔ m یک رابطهٔ هم‌ارزی است نتیجهٔ ساده‌ای از تعاریف مربوطه است. ردهٔ هم‌ارزی عدد صحیح a را با $\bar{a}$ نشان می‌دهیم و خاصیت (۲۰) را به یاد می‌آوریم که در این وضع می‌تواند به‌صورت زیر بیان شود:

$$\bar{a} = \bar{b} \iff a \equiv b \pmod m. \tag{۲۰′}$$

به‌ازای هر $a \in \mathbf{Z}$، اعداد صحیحی مانند q و r، با $0 \le r < m$، وجود دارند به‌طوری‌که $a = mq + r$. از اینرو، $a - r = mq$ و $a \equiv r \pmod m$؛ بنابراین، طبق (۲۰′)، $\bar{a} = \bar{r}$. چون a دلخواه بود و $0 \le r < m$، نتیجه می‌شود که هر ردهٔ هم‌ارزی باید یکی از $\bar{0},\bar{1},\bar{2},\bar{3},\ldots,(\overline{m-1})$ باشد. اما این m ردهٔ هم‌ارزی متمایزند؛ زیرا هرگاه $0 \le i < j < m$، آنگاه $0 < (j-i) < m$ و $m \nmid (j-i)$. لذا، $i \not\equiv j \pmod m$؛ و در نتیجه، طبق (۲۰′)، $\bar{i} \neq \bar{j}$. بنابراین، درست m ردهٔ هم‌ارزی وجود دارد.

(دو) $m \mid a-b$ و $m \mid c-d$ داده شده‌اند. از اینرو، m

$$(a-b)+(c-d) = (a+c)-(b+d)$$

را عاد می‌کند؛ ولذا $a+c \equiv b+d \pmod m$. به‌همین‌نحو، m، $(a-b)c + (c-d)b$،

و درنتیجه

$$ac - bc + cb - db = ac - bd$$

را عاد می‌کند ؛ لذا ، $ac \equiv bd \pmod m$.

(سه) چون $ab \equiv ac \pmod m$ ، $m \mid a(b-c)$. وچون $(m,a) = 1$ ، بنابر قضیهٔ ۶.۶ ، $m \mid b - c$ ؛ و لذا ، $b \equiv c \pmod m$.

۷ اصل انتخاب ، ترتیب ، ولم‌زرن[1]

تذکر. دراین بخش فقط با **مجموعه‌ها** سر و کار داریم . هیچ ردهٔ حقیقی در کار نخواهد آمد .

هرگاه $I \neq \varnothing$ و $\{A_i \mid i \in I\}$ خانواده‌ای از مجموعه‌ها باشد به طوری که به‌ازای هر $i \in I$ ، $A_i \neq \varnothing$ ، آنگاه می‌خواهیم بدانیم آیا $\coprod_{i \in I} A_i \neq \varnothing$. ثابت شده است که این نتیجهٔ ظاهرا" بی‌ضرر را نمی‌توان از اصول موضوع نظریهٔ مجموعه‌ها (با آنکه با آنها ناسازگار نیست ؛ ر.ک. پی . ج . کوهن[2] [۵۹]) به دست آورد . درنتیجه ، اصل موضوع زیر را می‌پذیریم .

اصل انتخاب . حاصلضرب هر خانواده از مجموعه‌های ناتهی که به وسیلهٔ یک مجموعهٔ ناتهی اندیسگذاری شده است ناتهی است .

برای‌صورت دیگری‌ازاصل انتخاب ، ر.ک. تمرین ۴ . دو گزاره معادل اصل انتخاب وجود دارند که در اثبات چند قضیهٔ مهم اساسی‌اند . برای بیان این گزاره‌های معادل باید چند مفهوم دیگر را معرفی کنیم .

یک **مجموعهٔ جزئی مرتب** مجموعه‌ای است ناتهی مانند A همراه با رابطه‌ای چون R بر $A \times A$ (به‌نام **ترتیب جزئی** از A) که منعکس و متعدی است (ر.ک. روابط (۱۵) و (۱۷) در بخش ۴) و

---

1. Zorn
2. P. J. Cohen

(۳۱) $(a,b)\in R \ \text{و}\ (b,a)\in R \Rightarrow a=b$: **پاد متقارن**

هرگاه R یک ترتیب جزئی از A باشد، آنگاه معمولاً به جای $(a,b)\in R$ می‌نویسیم $a\le b$. با این نماد، شرایط (۱۵)، (۱۷)، و (۳۱) (به‌ازای هر $a,b,c\in A$) خواهند شد:

$$a\le a;$$

$$a\le b \ \text{و}\ b\le c \Rightarrow a\le c;$$

$$a\le b \ \text{و}\ b\le a \Rightarrow a=b.$$

اگر $a\le b$ و $a\ne b$، می‌نویسیم $a<b$.

عنصرهای $a,b\in A$ را **قابل مقایسه** گویند اگر $a\le b$ یا $b\le a$. دو عنصر یک مجموعهٔ جزئی مرتب لزوماً قابل مقایسه نیستند. یک ترتیب جزئی از مجموعهٔ A که هر دو عنصرش قابل مقایسه باشند یک **ترتیب خطی** (یا **کلی** یا **ساده**) نامیده می‌شود.

مثال. فرض کنیم A مجموعهٔ توان (مجموعهٔ جمیع زیرمجموعه‌های) $\{1,2,3,4,5\}$ باشد. تعریف می‌کنیم $C\le D$ اگر و فقط اگر $C\subset D$. A جزئی مرتب است، اما خطی مرتب نیست (مثلاً، $\{1,2\}$ و $\{3,4\}$ قابل مقایسه نیستند).

فرض کنیم $(A,\le)$ یک مجموعهٔ جزئی مرتب باشد. عنصر $a\in A$ در A **ماکزیمال** است اگر به ازای هر $c\in A$، که **با a قابل مقایسه باشد**، $c\le a$؛ به عبارت دیگر، به‌ازای هر $c\in A$، $a\le c\Rightarrow a=c$. توجه کنید که اگر a ماکزیمال باشد، لازم نیست به ازای هر $c\in A$، $c\le a$ (ممکن است $c\in A$ ای غیرقابل مقایسه با a وجود داشته باشد). به علاوه، یک مجموعه ممکن است عنصر ماکزیمال بسیار داشته باشد (تمرین ۵) یا اصلاً نداشته باشد (مثلاً، $\mathbf{Z}$ با ترتیب معمولی). یک **کران بالایی** زیر مجموعهٔ B از A عنصری است مانند $d\in A$ به‌طوری‌که به‌ازای هر $b\in B$، $b\le d$. زیرمجموعهٔ ناتهی B از A که با $\le$ خطی مرتب باشد یک **زنجیر** در A نام دارد.

لم زرن. *هرگاه A یک مجموعهٔ جزئی مرتب ناتهی باشد به‌طوری‌که هر زنجیر در A کران بالایی در A داشته باشد، آنگاه A شامل عنصر ماکزیمال است.*

با این فرض که جمیع اصول موضوع معمول دیگر نظریهٔ مجموعه‌ها برقرارند، می‌توان

ثابت کرد که لم زرن درست است اگر و فقط اگر اصل انتخاب برقرار باشد؛ یعنی، این دو اصل معادلند؛ ر.ک. ای. هیوویت[1] و کا. استرومبرگ[2] [۵۷، ص ۱۴] . لم زرن حربهٔ توانایی است و مکرر در آینده به کار خواهد رفت.

فرض کنیم B زیرمجموعه‌ای ناتهی از مجموعهٔ جزئی مرتب $(A,\leq)$ باشد. عنصر $c\in B$ **کوچکترین عنصر** (یا **مینیمم**) B است اگر به ازای هر $b\in B$ ، $c\leq b$. هرگاه هر زیرمجموعهٔ ناتهی A کوچکترین عنصر داشته باشد، آنگاه گویند A **خوش ترتیب** است. هر مجموعهٔ خوش ترتیب خطی مرتب است (ولی عکس آن درست نیست)، زیرا به‌ازای هر $a,b\in A$ ، زیرمجموعهٔ $\{a,b\}$ باید کوچکترین عنصر داشته باشد؛ یعنی، $a\leq b$ یا $b\leq a$. در اینجا حکم دیگری وجود دارد که می‌توان معادل بودنش را با اصل انتخاب ثابت کرد (ر.ک. ای. هیوویت و کا. استرومبرگ [۵۷، ص ۱۴]).

اصل خوش ترتیبی. هرگاه A یک مجموعهٔ ناتهی باشد، آنگاه یک ترتیب خطی مانند $\leq$ از A وجود دارد به طوری که $(A,\leq)$ خوش ترتیب است.

چند مثال. ما قبلا" فرض کرده‌ایم (بخش ۶) که مجموعهٔ اعداد طبیعی **N** خوش ترتیب است. مجموعهٔ جمیع اعداد صحیح **Z** با ترتیب معمولی اندازه خطی مرتب است ولی خوش ترتیب **نیست** (مثلا" ، زیرمجموعهٔ اعداد صحیح منفی کوچکترین عنصر ندارد) . اما هر یک از زیرمجموعه‌های زیر از **Z** خوش ترتیب است (که در آنها، طبق تعریف، a سمت چپ b است $\Leftrightarrow a<b$):

(یک) $0,1,-1,2,-2,3,-3,\ldots,n,-n,\ldots$ ؛

(دو) $0,1,3,5,7,\ldots,2,4,6,8,\ldots,-1,-2,-3,-4,\ldots$ ؛

(سه) $0,3,4,5,6,\ldots,-1,-2,-3,-4,\ldots,1,2$.

این ترتیبها کاملا" از یکدیگر متفاوتند. هر عنصر ناصفر a در ترتیب (یک) سابق بلافصل دارد (یعنی، عنصری مانند c هست به‌طوری‌که a کوچکترین عنصر در زیرمجموعهٔ $\{x\mid c<x\}$ است) . اما عناصر -1 و 2 در ترتیب (دو) و -1 و 1 در ترتیب (سه) سابق بلافصل ندارند. در ترتیبهای (یک) و (دو) عنصر ماکزیمال وجود ندارد، ولی

---

1. E. Hewitt 2. K. Stromberg

در ترتیب (سه) 2 عنصر ماکزیمال است . عنصر 0 کوچکترین عنصر در هر سه ترتیب است .

مزیت عمدهٔ اصل خوش ترتیبی در این است که به ما توان تعمیم اصل استقرای ریاضی برای اعداد صحیح مثبت (قضیهٔ ۱.۶) را به هر مجموعهٔ خوش ترتیب می‌دهد .

قضیهٔ ۱.۷ (اصل استقرای ترانسفینی) . *هرگاه* B *زیرمجموعهٔ مجموعهٔ خوش ترتیب* $(A,\leq)$ *باشد به طوری که به ازای هر* $a\in A$ ،

$$\{c\in A \mid c<a\}\subset B \Rightarrow a\in B,$$

آنگاه $B=A$.

برهان . هرگاه $A-B\neq\varnothing$ ، آنگاه کوچکترین عنصری مانند $a\in A-B$ وجود دارد . طبق تعاریف **کوچکترین عنصر** و $A-B$ ، باید داشته باشیم $\{c\in A \mid c<a\}\subset B$. در این صورت ، طبق فرض، $a\in B$ ؛ درنتیجه ، $B\cap(A-B)=\varnothing$ ، که یک تناقض است . بنابراین ، $A-B=\varnothing$ و $A=B$.

تمرینات

۱ . فرض کنید $(A,\leq)$ یک مجموعهٔ جزئی مرتب بوده و B زیرمجموعه‌ای ناتهی از آن باشد . یک ***کران پایینی*** B عنصری است مانند $d\in A$ به‌طوری‌که به ازای **هر** $b\in B$ ، $d\leq b$. ***بزرگترین کران پایینی*** B **(g.l.b.)** یک کران پایینی مانند d_0 از B است به‌طوری‌که به‌ازای هر کران پایینی دیگر d از B ، $d\leq d_0$. ***کوچکترین کران بالایی*** B **(l.u.b.)** یک کران بالایی مانند t_0 از B است به‌طوری‌که به‌ازای هر کران بالایی دیگر t از B ، $t_0\leq t$. $(A,\leq)$ یک **شبکه** است اگر به‌ازای هر $a,b\in A$ ، مجموعهٔ $\{a,b\}$ بزرگترین کران پایینی و کوچکترین کران بالایی داشته باشد .

(آ) هرگاه $S\neq\varnothing$ ، آنگاه مجموعهٔ توان $P(S)$ مرتب شده به وسیلهٔ شمول نظریهٔ مجموعه‌ها یک شبکه است ، که عنصر ماکزیمال منحصر به فرد دارد .

(ب) یک مجموعهٔ جزئی مرتب مثال بزنید که شبکه **نباشد** .

(پ) یک شبکهٔ بدون عنصر ماکزیمال و یک مجموعهٔ جزئی مرتب با دو عنصر

ماکزیمال مثال بزنید.

۲. شبکهٔ $(A,\leq)$ (ر.ک. تمرین ۱) را **تام** گویند اگر هر زیرمجموعهٔ ناتهی از A کوچکترین کران بالایی و بزرگترین کران پایینی داشته باشد. گویند یک نگاشت از مجموعه‌های جزئی مرتب مانند $f: A \to B$ ترتیب را حفظ می‌کند اگر $a \leq a'$ در A ایجاب کند که $f(a) \leq f(a')$ در B. ثابت کنید یک نگاشت حافظ ترتیب مانند f از شبکهٔ تام A به توی خود دست کم یک عنصر ثابت دارد (یعنی، عنصری مانند $a \in A$ هست به‌طوری‌که $f(a) = a$).

۳. خوش ترتیبی مجموعهٔ اعداد گویای $\mathbf{Q}$ را نشان دهید.

۴. فرض کنید S یک مجموعه باشد. یک ***تابع انتخاب*** برای S تابعی است مانند f از مجموعهٔ تمام زیر مجموعه‌های ناتهی S به S به‌طوری‌که به‌ازای هر $A \subset S$، $A \neq \varnothing$، $f(A) \in A$. نشان دهید که اصل انتخاب معادل آن است که بگوییم هر مجموعهٔ S دارای تابع انتخاب است.

۵. فرض کنید S مجموعهٔ تمام نقاط (x,y) در صفحه با خاصیت $y \geq 0$ باشد. یک ترتیب را با

$$(x_1,y_1) \leq (x_2,y_2) \Leftrightarrow y_1 \leq y_2 \quad \text{و} \quad x_1 = x_2$$

تعریف کنید. نشان دهید که این یک ترتیب جزئی از S است، و S بی‌نهایت عنصر ماکزیمال دارد.

۶. ثابت کنید هرگاه در خانواده‌ٔ $\{A_i \mid i \in I \neq \varnothing\}$ همهٔ مجموعه‌ها ناتهی باشند، آنگاه هریک از تصاویر $\pi_k : \prod_{i \in I} A_i \to A_k$ سورژکتیو است.

۷. فرض کنید $(A,\leq)$ یک مجموعهٔ خطی مرتب باشد. ***تالی بلافصل*** $a \in A$ (در صورت وجود) کوچکترین عنصر در مجموعهٔ $\{x \in A \mid a < x\}$ است. ثابت کنید هرگاه A به وسیلهٔ $\leq$ خوش ترتیب شده باشد، آنگاه حداکثر یک عنصر از A تالی بلافصل ندارد. یک مجموعهٔ خطی مرتب مثال بزنید که در آن درست دو عنصر تالی بلافصل نداشته باشند.

۸ اعداد اصلی

تعریف و خواص مقدماتی اعداد اصلی مکرر در آینده لازم خواهند شد. لیکن، تا پایان

این بخش (از قضیهٔ ۵۰۸ به بعد)، فقط گهگاه به کار می‌آیند (قضایای II ۰ ۲۰۱ و IV ۰ ۶۰۲؛ لم ۷ ۰ ۵۰۳؛ قضایای ۷ ۰ ۶۰۳ و VI ۰ ۹۰۱). در صورت تمایل، می‌توانید آن را فعلا" حذف کنید.

دو مجموعهٔ A و B را **همتوان** گویند اگر یک نگاشت بیژکتیو مانند $A \to B$ وجود داشته باشد. در این حالت می‌نویسیم $A \sim B$.

قضیهٔ ۱۰۸ ۰ *همتوانی یک رابطهٔ هم‌ارزی بر ردهٔ تمام مجموعه‌های S است.*

برهان. تمرین؛ توجه کنید که $\varnothing \sim \varnothing$، زیرا $\varnothing \times \varnothing \subset \varnothing$ یک رابطه است (که به طور خالی) یک تابع بیژکتیو است.[1]

فرض کنیم $I_0 = \varnothing$ و به‌ازای هر $n \in \mathbf{N}^*$، قرار می‌دهیم $I_n = \{1,2,3,\ldots,n\}$. اثبات اینکه I_m و I_n همتوان‌اند اگر و فقط اگر $m = n$ مشکل نیست (تمرین ۱). این سخن که مجموعهٔ A درست n عنصر دارد یعنی A و I_n همتوان‌اند؛ یعنی، A و I_n تحت رابطهٔ همتوانی در یک ردهٔ هم‌ارزی قرار دارند. به چنین مجموعهٔ A (که به‌ازای $n \geq 0$ ی منحصر به فرد، $A \sim I_n$) **متناهی** گویند؛ هر مجموعه که متناهی نباشد **نامتناهی** است. لذا، به‌ازای مجموعهٔ متناهی A، ردهٔ هم‌ارزی A تحت همتوانی جوابی به سوال زیر است: چند عنصر در A وجوددارند؟ این ملاحظات انگیزهٔ تعریف زیر می‌باشند.

تعریف ۲۰۸ ۰ *عدد اصلی* (یا *اصلیت*) مجموعهٔ A، که با $|A|$ نموده می‌شود، ردهٔ هم‌ارزی A تحت رابطهٔ هم‌ارزی همتوانی است. $|A|$، بسته به نامتناهی یا متناهی بودن مجموعهٔ A، یک عدد اصلی نامتناهی یا متناهی است.

اعداد اصلی با حروف کوچک یونانی α، β، γ، و غیره نیز نموده می‌شوند. به دلایلی که در بند پیش ذکر شد، عدد صحیح $n \geq 0$ را با عدد اصلی $|I_n|$ یکی گرفته و می‌نویسیم $n = |I_n|$؛ درنتیجه، عدد اصلی یک مجموعهٔ متناهی دقیقا" تعداد عناصر

---

۱. ر.ک. صفحهٔ ۸۰

آن مجموعه است.

اعداد اصلی را بعضی به نوعی متفاوت با ما تعریف می‌کنند، به این نحو که عدد اصلی در واقع مجموعه است (تا یک ردهٔ حقیقی مثل تعریف ۲۰۸). ما این تعریف را از دو جهت انتخاب کرده‌ایم که هم در وقت صرفه‌جویی کنیم و هم به این خاطر که مفهوم شهودی "تعداد عنصرهای یک مجموعه" بهتر منعکس گردد. اعداد اصلی، بی‌توجه به تعریف آنها، دارای خواص زیرند (دو تای اول، در حالت ما، نتایج فوری قضیهٔ ۱۰۸ و تعریف ۲۰۸ می‌باشند):

(یک) هر مجموعه عدد اصلی منحصر به فرد دارد؛

(دو) دومجموعه‌یک‌عدداصلی دارند اگروفقط اگر همتوان باشند $(|A| = |B| \Leftrightarrow A \sim B)$؛

(سه) عدد اصلی یک مجموعهٔ متناهی تعداد عناصر آن مجموعه است.

لذا، احکام در باب اعداد اصلی چیزی جز احکام در باب مجموعه‌های همتوان نیست.

مثال. عدد اصلی مجموعهٔ اعداد طبیعی $\mathbf{N}$ را معمولا "با $\aleph_0$ (بخوانید: "الف صفر") نشان می‌دهند. مجموعهٔ A با اصلیت $\aleph_0$ (یعنی، مجموعه‌ای همتوان با $\mathbf{N}$) **شمارشپذیر** نامیده می‌شود. مجموعهٔ $\mathbf{N}^*$، مجموعهٔ اعداد صحیح $\mathbf{Z}$، و مجموعهٔ اعداد گویای $\mathbf{Q}$ شمارشپذیرند (تمرین ۳)، اما مجموعهٔ اعداد حقیقی $\mathbf{R}$ شمارشپذیر **نیست** (تمرین ۹).

تعریف ۳۰۸. فرض کنیم α و β اعدادی اصلی باشند. **مجموع** $\alpha + \beta$ مساوی عدد اصلی $|\mathbf{A} \cup \mathbf{B}|$ تعریف می‌شود، که در آن $\mathbf{A}$ و $\mathbf{B}$ مجموعه‌هایی از هم جدایند به‌طوری که $|\mathbf{A}| = \alpha$ و $|\mathbf{B}| = \beta$. ***حاصل‌ضرب*** $\alpha\beta$ مساوی عدد اصلی $|\mathbf{A} \times \mathbf{B}|$ تعریف می‌شود.

از هم جدا بودن A و B در تعریف حاصل‌ضرب $\alpha\beta$ عملا "لازم نیست (تمرین ۴). طبق تعریف عدد اصلی α، همواره مجموعه‌ای مانند A هست به‌طوری‌که $|A| = \alpha$. به آسانی تحقیق می‌شود که مجموعه‌های *از هم جدا*، که در تعریف $\alpha + \beta$ لازمند، همیشه وجود داشته و مجموع $\alpha + \beta$ و حاصل‌ضرب $\alpha\beta$ از انتخاب مجموعه‌های A,B مستقل است (تمرین ۴). جمع و ضرب اعداد اصلی شرکتپذیر و تعویضپذیرند، و قوانین پخشپذیری برقرارند (تمرین ۵). به علاوه، جمع و ضرب اعداد اصلی متناهی با جمع و ضرب اعداد صحیح نامنفی که با آنها یکی شده‌اند یکسان‌اند؛ زیرا هرگاه A دارای m عنصر و B دارای

n عنصر بوده و $A \cap B = \varnothing$ ، آنگاه $A \cup B$ دارای $m+n$ عنصر و $A \times B$ دارای mn عنصر می‌باشد (برای دقت بیشتر، ر.ک. تمرین ۶).

تعریف ۴.۸ . فرض کنیم α,β اعدادی اصلی بوده و A,B مجموعه‌هایی باشند به‌طوری‌که $|A| = \alpha, |B| = \beta$. α ***کوچکتر یا مساوی*** β است، و با $\alpha \leq \beta$ یا $\beta \geq \alpha$ نموده می‌شود، اگر A با زیـر مجموعه‌ای از B همتوان باشد (یعنی، یک نگاشت انژکتیو مانند $A \to B$ وجود داشته بـاشد) . α ***اکیدا "کوچکتر از*** β است، و با $\alpha < \beta$ یا $\beta > \alpha$ نموده می‌شود، اگر $\alpha \leq \beta$ و $\alpha \neq \beta$.

به آسانی تحقیق می‌شود که تعریف $\leq$ به انتخاب A و B بستگی ندارد (تمرین ۷) . در قضیهٔ ۷.۸ نشـان داده‌ایم که ردهٔ تمام اعداد اصلی با $\leq$ خطی مرتب است. برای اعداد اصلی متناهی، $\leq$ با ترتیب معمولی اعداد صحیح نامنفی یکی است (تمرین ۱) . این امر که بزرگترین عدد اصلی وجود ندارد نتیجه‌ای است فوری از قضیهٔ زیر.

قضیهٔ ۵.۸ . ***هرگاه*** A ***یک مجموعه و*** $P(A)$ ***مجموعهٔ توان باشد، آنگاه*** $|A| < |P(A)|$.

طرح برهان. ارتباط $a \mapsto \{a\}$ معـرف یـک نـگاشت انـژکتیو $A \to P(A)$ است؛ و لذا، $|A| \leq |P(A)|$. هرگـاه یک نـگاشت بیژکتیو مانند $f: A \to P(A)$ وجود می‌داشت، آنگاه به‌ازای $a_0 \in A$ ی، $f(a_0) = B$ ، که در آن $B = \{a \in A \mid a \notin f(a)\} \subset A$. ولی این تناقض به بار می‌آورد: $a_0 \in B$ و $a_0 \notin B$. بنـابراین، $|A| \neq |P(A)|$؛ و در نتیجه، $|A| < |P(A)|$.

تبصره. بنابرقضیهٔ ۵.۸، $\aleph_0 = |\mathbf{N}| < |P(\mathbf{N})|$. می‌توان نشان داد که $|P(\mathbf{N})| = |\mathbf{R}|$ ، که در آن $\mathbf{R}$ مجموعهٔ اعداد حقیقی است. این حدس که عددی اصلی مانند β نیست که $\aleph_0 < \beta < |P(\mathbf{N})| = |\mathbf{R}|$ ***فرض پیوستار*** نـام دارد. ثابت شده است که این فرض از اصل انتخاب و سایر اصول اساسی نظریهٔ مجموعه‌ها مستقل است؛ ر.ک. پی. ج. کوهن [۵۹] .

تا آخر این بخش به ذکر چند نکته که در چند مرحله در آینده ضرورت دارند اختصاص یافته است (ر.ک. اولین بند این بخش).

قضیهٔ ۶۰۸ (شرودر[1] ــ برنشتاین[2]). *هرگاه A و B مجموعه‌هایی باشند به‌طوری‌که* $|A| \leq |B|$ *و* $|B| \leq |A|$، *آنگاه* $|A| = |B|$.

طرح برهان. طبق فرض، نگاشتهای انژکتیو $f: A \to B$ و $g: B \to A$ وجود دارند. f و g را در ساختن یک بیژکسیون $h: A \to B$ به کار می‌بریم. این ایجاب خواهد کرد که $A \sim B$؛ و درنتیجه، $|A| = |B|$. هرگاه $a \in A$، آنگاه چون g انژکتیو است، مجموعهٔ $g^{-1}(a)$ یا تهی است (که در این حالت گوییم a بی‌تبار است) یا فقط از یک عنصر $b \in B$ تشکیل شده است (که در این حالت می‌نویسیم $g^{-1}(a) = b$ و گوییم b ***تبار*** a است). به همین نحو، به‌ازای $b \in B$، یا داریم $f^{-1}(b) = \varnothing$ (b ***بی‌تبار است***) یا $f^{-1}(b) = a' \in A$ (a' ***تبار*** b است). اگر "نیای" عنصر $a \in A$ را به این‌نحو تعقیب کنیم، یکی از سه صورت زیر رخ می‌دهد. یا به عنصر بی‌تباری در A می‌رسیم (یک ***نیای*** $a \in A$)، یا به عنصر بی‌تباری در B می‌رسیم (یک ***نیای*** a)، یا نیای $a \in A$ را می‌توان همین‌طور تعقیب کرد (***بی‌نهایت نیا***). حال سه زیرمجموعه از A [یا B] را به صورت زیر تعریف می‌کنیم:

$$A_1 = \{a \in A \mid a \text{ یک نیای بی‌تبار در } A \text{ دارد}\}$$
$$A_2 = \{a \in A \mid a \text{ یک نیای بی‌تبار در } B \text{ دارد}\}$$
$$A_3 = \{a \in A \mid a \text{ بی‌نهایت نیا دارد}\}$$
$$B_1 = \{b \in B \mid b \text{ یک نیای بی‌تبار در } A \text{ دارد}\}$$
$$B_2 = \{b \in B \mid b \text{ یک نیای بی‌تبار در } B \text{ دارد}\}$$
$$B_3 = \{b \in B \mid b \text{ بی‌نهایت نیا دارد}\}$$

تحقیق کنید که A_i ها [B_i ها] دو به دو از هم جدایند، اجتماع این مجموعه‌ها مساوی A [B] است، به‌ازای $i = 1, 3$، $f \mid A_i$ یک بیژکسیون $A_i \to B_i$ است، و $g \mid B_2$ یک بیژکسیون $B_2 \to A_2$ می‌باشد. در نتیجه، نگاشت $h: A \to B$ داده شده به صورت زیر یک بیژکسیون است:

$$h(a) = \begin{cases} f(a) & \text{اگر } a \in A_1 \cup A_3 \\ g^{-1}(a) & \text{اگر } a \in A_2 \end{cases}$$

---

1. Schroeder
2. Bernstein

قضیهٔ ۷۰۸ . *ردهٔ تمام اعداد اصلی با $\leq$ به‌طور خطی مرتب شده است . هرگاه α و β اعدادی اصلی باشند ، درست یکی از روابط زیر برقرار است :*

$$\alpha < \beta; \quad \alpha = \beta; \quad \beta < \alpha \quad \text{(قانون تثلیث)}$$

طرح برهان . به آسانی تحقیق می‌شود که $\leq$ یک ترتیب جزئی است . فرض کنیم α,β اعدادی اصلی بوده و A,B مجموعه‌هایی باشند که داشته باشیم $|A| = \alpha, |B| = \beta$. با اعمال لم زرن بر مجموعهٔ $\mathfrak{F}$ مرکب از تمام جفتهای (f,X) ، که $X \subset A$ و $f: X \to B$ یک نگاشت انژکتیو است ، نشان می‌دهیم که $\leq$ یک ترتیب خطی است (یعنی ، $\alpha \leq \beta$ یا $\beta \leq \alpha$) . تحقیق کنید که $\mathfrak{F} \neq \varnothing$ و ترتیب داده شده با $(f_1,X_1) \leq (f_2,X_2)$ اگر و فقط اگر $X_1 \subset X_2$ و $f_2 | X_1 = f_1$ یک ترتیب جزئی از $\mathfrak{F}$ است . اگر $\{(f_i,X_i) \mid i \in I\}$ یک زنجیر در $\mathfrak{F}$ باشد ، قرار می‌دهیم $X = \bigcup_{i \in I} X_i$ ، و $f: X \to B$ را به‌ازای $x \in X_i$ با $f(x) = f_i(x)$ تعریف می‌کنیم . نشان دهید که f یک نگاشت انژکتیو است ، و (f,X) یک کران بالایی زنجیر داده‌شده در $\mathfrak{F}$ می‌باشد . لذا ، طبق لم زرن ، یک عنصر ماکزیمال مانند (g,X) از $\mathfrak{F}$ وجود دارد . حکم می‌کنیم که $X = A$ یا $\operatorname{Im} g = B$. چرا که اگر هردوی اینها نادرست بودند ، می‌شد $a \in A - X$ ای و $b \in B - \operatorname{Im} g$ ای یافت و نگاشت انژکتیو $h: X \cup \{a\} \to B$ را با $h(x) = g(x)$ به‌ازای $x \in X$ و $h(a) = b$ تعریف کرد . در این‌صورت ، $(h,X \cup \{a\}) \in \mathfrak{F}$ و $(g,X) < (h,X \cup \{a\})$ ، که با ماکزیمال بودن (g,X) متناقض است . بنابراین ، یا $X = A$ ؛ درنتیجه ، $|B| \leq |A|$ ، یا $\operatorname{Im} g = B$ ، که در این حالت نگاشت انژکتیو $B \xrightarrow{g^{-1}} X \subset A$ نشان می‌دهد که $|A| \leq |B|$. با استفاده از این مطالب ، قضیهٔ شرودر ـ برنشتاین ۶۰۸ ، و تعریف ۴۰۸ ، قانون تثلیث را ثابت کنید .

چند تبصره . گوییم یک خانواده از توابع جزئی مرتب همانند در برهان قضیهٔ ۷۰۸ *به وسیلهٔ توسیع مرتب شده‌است* . برهان این قضیه یک مثال نوعی از کاربرد لم زرن است . استدلالهای مشابه در آینده اغلب به اختصار بیان خواهند شد .

قضیهٔ ۸۰۸ . *هر مجموعهٔ نامتناهی زیرمجموعه‌ای شمارشپذیر دارد . بخصوص ، به‌ازای هر عدد اصلی نامتناهی α ، $\aleph_0 \leq \alpha$.*

طرح برهان. هرگاه B یک زیرمجموعهٔ متناهی از مجموعهٔ نامتناهی A باشد، آنگاه $A - B$ ناتهی است. به‌ازای هر زیرمجموعهٔ متناهی B از A، عنصری مانند $x_B \in A - B$ انتخاب می‌کنیم (اصل انتخاب). فرض کنیم F مجموعهٔ تمام زیرمجموعه‌های متناهی A بوده و نگاشت $f: F \to F$ را با $f(B) = B \cup \{x_B\}$ تعریف می‌کنیم. $a \in A$ را اختیار می‌نماییم. طبق قضیهٔ بازگشتی ۲۰۶ (با $f_n = f$ به‌ازای هر n)، تابعی مانند $\varphi: \mathbf{N} \to F$ هست به‌طوری‌که

$$\varphi(0) = \{a\} \text{ و } \varphi(n+1) = f(\varphi(n)) = \varphi(n) \cup \{x_{\varphi(n)}\} \ (n \geq 0).$$

فرض کنیم $g: \mathbf{N} \to A$ تابع تعریف شده با

$$g(0) = a; g(1) = x_{\varphi(0)} = x_{\{a\}}; \ldots; g(n+1) = x_{\varphi(n)}; \ldots$$

باشد. با استفاده از خواص ترتیب $\mathbf{N}$ و مطالب زیر، تحقیق کنید که g انژکتیو است:

(یک) به‌ازای هر $n \geq 0$، $g(n) \in \varphi(n)$؛

(دو) به‌ازای هر $n \geq 1$، $g(n) \notin \varphi(n-1)$؛

(سه) به‌ازای هر $m < n$، $g(n) \notin \varphi(m)$.

بنابراین، $\operatorname{Im} g$ زیر مجموعه‌ای از A است به‌طوری‌که $|\operatorname{Im} g| = |\mathbf{N}| = \aleph_0$.

لم ۹۰۸. *هرگاه A یک مجموعهٔ نامتناهی بوده و F مجموعه‌ای متناهی باشد، آنگاه $|A \cup F| = |A|$. بخصوص، به‌ازای هر عدد اصلی نامتناهی α و هر عدد طبیعی (اصلی متناهی) n، $\alpha + n = \alpha$.*

طرح برهان. کافی است فرض کنیم $A \cap F = \varnothing$ (F را در صورت لزوم با $F - A$ عوض می‌کنیم). هرگاه $F = \{b_1, b_2, \ldots, b_n\}$ و $D = \{x_i \mid i \in \mathbf{N}^*\}$ یک زیرمجموعهٔ شمارشپذیر از A باشد (قضیهٔ ۸۰۸)، تحقیق کنید $f: A \to A \cup F$ یک بیژکسیون است، که در آن f به صورت زیر داده می‌شود:

$$f(x) = \begin{cases} b_i & \text{به ازای } x = x_i, 1 \leq i \leq n \\ x_{i-n} & \text{به ازای } x = x_i, i > n \\ x & \text{به ازای } x \in A - D \end{cases}$$

قضیهٔ ۱۰۰۸. *هرگاه α و β اعدادی اصلی باشند به‌طوری‌که $\alpha \leq \beta$ و α نامتناهی*

باشد، آنگاه $\alpha + \beta = \alpha$.

طرح برهان. کافی است ثابت کنیم $\alpha + \alpha = \alpha$ (فقط تحقیق کنیم که $\alpha + \alpha = \alpha \leq \alpha + \beta \leq \alpha$ و با اعمال قضیهٔ شرودر ـ برنشتاین نتیجه بگیریم که $\alpha + \beta = \alpha$). فرض کنیم A مجموعه‌ای با $|A| = \alpha$ بوده و $\mathfrak{F}$ مجموعهٔ تمام جفتهای (f,X) باشد، که در آن $X \subset A$ و $f : X \times \{0,1\} \to X$ یک بیژکسیون است. $\mathfrak{F}$ را به وسیلهٔ توسیع (مثل برهان قضیهٔ ۷۰۸) جزئی مرتب کرده و تحقیق کنید که مفروضات لم زرن برقرارند. تنها مشکل نشان دادن این است که $\mathfrak{F} \neq \varnothing$. برای این کار توجه کنید که نگاشت $\mathbf{N} \times \{0,1\} \to \mathbf{N}$ داده شده با $(n,0) \mapsto 2n$ و $(n,1) \mapsto 2n+1$ بیژکسیون است. با استفاده از این امر، بیژکسیون $f : D \times \{0,1\} \to D$ را می‌سازیم، که در آن D یک زیرمجموعهٔ شمارشپذیر از A است (یعنی، $|D| = |\mathbf{N}|$ ؛ ر.ک. قضیهٔ ۸۰۸). لذا، طبق لم زرن، یک عنصر ماکزیمال مانند $(g,C) \in \mathfrak{F}$ وجود دارد.

واضح است که $C_0 = \{(c,0) \mid c \in C\}$ و $C_1 = \{(c,1) \mid c \in C\}$ مجموعه‌هایی از هم جدایند به‌طوری‌که $|C_0| = |C| = |C_1|$ و $C \times \{0,1\} = C_0 \cup C_1$. نگاشت $g : C \times \{0,1\} \to C$ یک بیژکسیون است. بنابراین، طبق تعریف ۳۰۸،

$$|C| = |C \times \{0,1\}| = |C_0 \cup C_1| = |C_0| + |C_1| = |C| + |C|.$$

برای اتمام برهان نشان خواهیم داد که $|C| = \alpha$. اگر $A - C$ نامتناهی می‌بود، طبق قضیهٔ ۸۰۸، شامل زیرمجموعهٔ شمارشپذیری مانند B می‌شد، و مثل بالا، یک بیژکسیون مانند $\xi : B \times \{0,1\} \to B$ وجود می‌داشت. دراین‌صورت، از تلفیق ξ با g یک‌بیژکسیون مانند

$$h : (C \cup B) \times \{0,1\} \to C \cup B$$

ساخته می‌شد به‌طوری‌که $(g,C) < (h, C \cup B) \in \mathfrak{F}$، که‌ماکزیمال‌بودن (g,C) را نقض می‌کرد. لذا، $A - C$ باید متناهی باشد. چون A نامتناهی است و $A = C \cup (A - C)$، C نیز باید نامتناهی باشد. بنابراین، طبق لم ۹۰۸، $|C| = |C \cup (A - C)| = |A| = \alpha$.

قضیهٔ ۱۱۰۸. *هرگاه α و β اعدادی اصلی باشند به‌طوری‌که $0 \neq \beta \leq \alpha$ و α نامتناهی است، آنگاه $\alpha\beta = \alpha$ ؛ بخصوص، $\alpha\aleph_0 = \alpha$ و اگر β متناهی باشد، $\aleph_0\beta = \aleph_0$.*

طرح برهان. چون $\alpha \leq \alpha\beta \leq \alpha\alpha$ ، کافی است (مثل برهان قضیهٔ ۱۰۰۸) ثابت کنیم $\alpha\alpha = \alpha$. فرض کنیم A یک مجموعهٔ نامتناهی با $|A| = \alpha$ بوده و $\mathfrak{F}$ مجموعهٔ تمام بیژکسیونهای $f: X \times X \to X$ باشد، که در آن X زیرمجموعه‌ای نامتناهی از A است. برای نشان دادن $\mathfrak{F} \neq \varnothing$ ، از اینکه A زیرمجموعهٔ شمارشپذیری مانند D دارد (در نتیجه، $|D| = |\mathbf{N}| = |\mathbf{N}^*|$) و نگاشت $(m,n) \mapsto 2^{m-1}(2n-1)$ داده‌شده با $\mathbf{N}^* \times \mathbf{N}^* \to \mathbf{N}^*$ یک بیژکسیون است استفاده کنید. $\mathfrak{F}$ را به وسیلهٔ توسیع جزئی مرتب کرده و، با استفاده از لم زرن، یک عنصر ماکزیمال مانند $g: B \times B \to B$ به دست آورید. بنابر تعریف g ، $|B||B| = |B \times B| = |B|$. برای اتمام برهان، نشان خواهیم داد که $|B| = |A| = \alpha$.

فرض کنیم $|A - B| > |B|$. بنابر قضیهٔ ۴۰۸، زیرمجموعه‌ای مانند C از $A - B$ هست به‌طوری‌که $|C| = |B|$. تحقیق کنید که

$$|C| = |B| = |B \times B| = |B \times C| = |C \times B| = |C \times C|$$

و این مجموعه‌ها دو به دو از هم جدایند. درنتیجه، بنابر تعریف ۳۰۸ و قضیهٔ ۱۰۰۸،

$$|(B \cup C) \times (B \cup C)| = |(B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C)|$$

$$= |B \times B| + |B \times C| + |C \times B| + |C \times C| = (|B| + |B|) + (|C| + |C|) = |B| + |C| = |B \cup C|$$

و یک بیژکسیون مانند $(B \cup C) \times (B \cup C) \to (B \cup C)$ هست، که با ماکزیمال بودن g در $\mathfrak{F}$ تعارض دارد. لذا، طبق قضایای ۷۰۸ و ۱۰۰۸ ، $|A - B| \leq B$ و

$$|B| = |A - B| + |B| = |(A - B) \cup B| = |A| = \alpha.$$

قضیهٔ ۱۲۰۸ . *فرض کنیم A یک مجموعه بوده و به‌ازای هر عدد صحیح $n \geq 1$ ،* $A^n = A \times A \times \cdots \times A$ *(n عامل).*

(یک) *هرگاه A متناهی باشد، آنگاه* $|A^n| = |A|^n$ *، و هرگاه A نامتناهی باشد، آنگاه* $|A^n| = |A|$.

(دو) $\left|\bigcup_{n \in \mathbf{N}^*} A^n\right| = \aleph_0 |A|$.

طرح برهان. (یک) بدیهی است اگر $|A|$ متناهی باشد، و در صورت نامتناهی بودن $|A|$ ، می‌توان آن را به‌استقرا بر n ثابت کرد (حالت $n = 2$ در قضیهٔ ۱۱۰۸ آمده است).

(دو) مجموعه‌های A^n $(n \geq 1)$ دو به‌دو از هم جدایند. هرگاه A نامتناهی باشد، آنگاه،

طبق (یک)، به‌ازای هر n یک بیژکسیون مانند $f_n : A^n \to A$ وجود دارد. نگاشت $\bigcup_{n\in\mathbf{N}^*} A^n \to \mathbf{N}^* \times A$، که $u \in A^n$ را به $(n, f_n(u))$ می‌نگارد، یک بیژکسیون است. بنابراین،

$$|\bigcup_{n\in\mathbf{N}^*} A^n| = |\mathbf{N}^* \times A| = |\mathbf{N}^*||A| = \aleph_0|A|.$$

اگر $A = \varnothing$، (دو) به وضوح درست است. لذا، فرض می‌کنیم A ناتهی و متناهی باشد. در این صورت، هر A^n ناتهی است و ساده‌است نشان دهیم که $\aleph_0 = |\mathbf{N}^*| \leq |\bigcup_{n\in\mathbf{N}^*} A^n|$. به علاوه، هر A^n متناهی است و به‌ازای هر n یک نگاشت انژکتیو مانند $g_n : A^n \to \mathbf{N}^*$ وجود دارد. نگاشت $\bigcup_{n\in\mathbf{N}^*} A^n \to \mathbf{N}^* \times \mathbf{N}^*$، که $u \in A^n$ را به $(n, g_n(u))$ می‌نگارد، انژکتیو است به‌طوری‌که، بنابر قضیهٔ ۱۱۰۸،

$$|\bigcup_{n\in\mathbf{N}^*} A^n| \leq |\mathbf{N}^* \times \mathbf{N}^*| = |\mathbf{N}^*| = \aleph_0$$

لذا، طبق قضیهٔ شرودر ــ برنشتاین، $|\bigcup_{n\in\mathbf{N}^*} A^n| = \aleph_0$. اما $\aleph_0 = \aleph_0|A|$، زیرا A متناهی است (قضیهٔ ۱۱۰۸).

نتیجهٔ ۱۳۰۸. *هرگاه A یک مجموعهٔ نامتناهی بوده و $F(A)$ مجموعهٔ تمام زیرمجموعه‌های متناهی از A باشد، آنگاه $|F(A)| = |A|$.*

برهان. نگاشت $A \to F(A)$ داده‌شده با $a \mapsto \{a\}$ انژکتیو است؛ درنتیجه، $|A| \leq |F(A)|$. به‌ازای هر زیرمجموعهٔ n عنصری S از A، $(a_1, \ldots, a_n) \in A^n$ را طوری اختیار می‌کنیم که $S = \{a_1, \ldots, a_n\}$. این یک نگاشت انژکتیو مانند $F(A) \to \bigcup_{n\in\mathbf{N}^*} A^n$ تعریف می‌کند که طبق قضایای ۱۱۰۸ و ۱۲۰۸، $|F(A)| \leq |\bigcup_{n\in\mathbf{N}^*} A^n| = \aleph_0|A| = |A|$. بنابراین، طبق قضیهٔ شرودر ــ برنشتاین ۶۰۸، $|A| = |F(A)|$.

تمرینات

۱. فرض کنید $I_0 = \varnothing$ و به‌ازای هر $n \in \mathbf{N}^*$، $I_n = \{1, 2, 3, \ldots, n\}$.

(آ) I_n با هیچ زیرمجموعهٔ حقیقی خود همتوان نیست [**راهنمایی.** استقرا] .

(ب) I_m و I_n همتوان‌اند اگر و فقط اگر $m = n$.

(پ) I_m با زیرمجموعه‌ای از I_n همتوان است ولی I_n با هیچ زیرمجموعه‌ای از I_m همتوان نیست اگر و فقط اگر $m < n$.

۲ . (آ) هر مجموعهٔ نامتناهی با یکی از زیرمجموعه‌های حقیقی خود همتوان است.

(ب) یک مجموعه متناهی است اگر و فقط اگر با هیچ‌زیرمجموعهٔ حقیقی‌خودهمتوان نباشد [ر.ک. تمرین ۱] .

۳ . (آ) $\mathbf{Z}$ یک مجموعهٔ شمارشپذیر است .

(ب) مجموعهٔ اعداد گویای $\mathbf{Q}$ شمارشپذیر است . [**راهنمایی.** نشان دهید که $|\mathbf{Z}| \leq |\mathbf{Q}| \leq |\mathbf{Z} \times \mathbf{Z}| = |\mathbf{Z}|$].

۴ . هرگاه A,A',B,B' مجموعه‌هایی باشند به‌طوری‌که $|A| = |A'|$ و $|B| = |B'|$ ، آنگاه $|A \times B| = |A' \times B'|$. هرگاه، علاوه بر این، $A \cap B = \varnothing = A' \cap B'$ ، آنگاه $|A \cup B| = |A' \cup B'|$. لذا، ضرب و جمع اعداد اصلی تعریف شده است .

۵ . به ازای هر سه عدد اصلی α,β,γ ،

(آ) $\alpha + \beta = \beta + \alpha$ و $\alpha\beta = \beta\alpha$ (قوانین تعویضپذیری) ؛

(ب) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ و $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (قوانین شرکتپذیری) ؛

(پ) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ و $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ (قوانین پخشپذیری) ؛

(ت) $\alpha + 0 = \alpha$ و $\alpha 1 = \alpha$.

(ث) هرگاه $\alpha \neq 0$ ، آنگاه β ای نیست که $\alpha + \beta = 0$ ، و هرگاه $\alpha \neq 1$ ، آنگاه β ای نیست که $\alpha\beta = 1$. لذا، تفریق و تقسیم اعداد اصلی قابل تعریف نیست .

۶ . فرض کنید I_n مثل تمرین 1 باشد. هرگاه $A \sim I_m$ و $B \sim I_n$ و $A \cap B = \varnothing$ ، آنگاه $(A \cup B) \sim I_{m+n}$ و $A \times B \sim I_{mn}$. لذا، هرگاه $|A|$ را با m و $|B|$ را با n یکی بگیریم ، آنگاه $|A| + |B| = m + n$ و $|A||B| = mn$.

۷ . هرگاه $A \sim A'$ ، $B \sim B'$ ، و $f: A \to B$ انژکتیو باشد ، آنگاه یک نگاشت انژکتیو مانند $A' \to B'$ وجود دارد . بنابراین ، رابطهٔ $\leq$ بر اعداد اصلی تعریف شده است .

۸ . هر زیرمجموعهٔ نامتناهی از یک مجموعهٔ شمارشپذیر شمارشپذیر است .

۹ . مجموعهٔ نامتناهی اعداد حقیقی $\mathbf{R}$ شمارشپذیر نیست (یعنی ، $\aleph_0 < |\mathbf{R}|$) . [**راهنمایی.** طبق تمرین ۸ ، کافی است نشان دهید که بازهٔ باز $(0,1)$ شمارشپذیر

نیست . فرض کنید هر عدد حقیقی را بتوان به صورت یک اعشاری نامتناهی نوشت. اگر (0,1) شمارشپذیر باشد ، یک بیژکسیون مانند بیژکسیون $f:\mathbf{N}^* \to (0,1)$ وجود دارد . اعشاری نامتناهی (عدد حقیقی) $\cdot a_1a_2\cdots$ در (0,1) را طوری بسازید که a_n رقم n ام بسط اعشاری $f(n)$ نباشد . این عدد نمی‌تواند در $\operatorname{Im} f$ باشد .]

۱۰ . اگر α,β اعداد اصلی باشند ، α^β را عدد اصلی مجموعهٔ تمام توابع $B \to A$ تعریف کنید ، که در آن A,B مجموعه‌هایی هستند که $|A| = \alpha, |B| = \beta$.

(آ) α^β از انتخاب A,B مستقل است .

(ب) $\alpha^{\beta+\gamma} = (\alpha^\beta)(\alpha^\gamma); (\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma); \alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$.

(پ) هرگاه $\beta \le \alpha$ ، آنگاه $\alpha^\gamma \le \beta^\gamma$.

(ت) هرگاه α,β متناهی با خاصیت $\alpha > 1, \beta > 1$ بوده و γ نامتناهی باشد ، آنگاه $\alpha^\gamma = \beta^\gamma$.

(ث) به‌ازای هر عدد اصلی متناهی n ، $\alpha^n = \alpha\alpha\cdots\alpha$ (n عامل) . از اینرو ، اگر α نامتناهی باشد ، $\alpha^n = \alpha$.

(ج) هرگاه $P(A)$ مجموعهٔ توان مجموعهٔ A باشد ، آنگاه $|P(A)| = 2^{|A|}$.

۱۱ . هرگاه I مجموعه‌ای نامتناهی بوده و به ازای هر $i \in I$ ، A_i مجموعه‌ای متناهی باشد ، آنگاه $|\bigcup_{i\in I} A_i| \le |I|$.

۱۲ . فرض کنید α عدد اصلی ثابتی بوده و به ازای هر $i \in I$ ، A_i مجموعه‌ای با خاصیت $|A_i| = \alpha$ باشد . در این صورت ، $|\bigcup_{i\in I} A_i| \le |I|\alpha$.

۱
گروهها

مفهوم گروه درجبراز اهمیتی اساسی برخوردار است. گروههایی که از حیث ساختار جبری یکی هستند یکریخت نامیده می‌شوند. هدف غایی در بررسی گروهها رده‌بندی تمام گروهها با تقریب یکریختی است، که در عمل یعنی یافتن شرایط لازم و کافی برای آنکه دو گروه یکریخت باشند. در حال حاضر امید کمی برای رده‌بندی گروههای دلخواه وجود دارد. لیکن می‌توان قضایای ساختاری کاملی برای رده‌های محدود مختلفی از گروهها، نظیر گروههای دوری (بخش ۳)، گروههای آبلی با تولید متناهی (بخش II ۲۰)، گروههای صادق در شرایط زنجیری (بخش II ۳۰)، و گروههای متناهی از مرتبهٔ کوچک (بخش II ۶۰) به دست آورد. برای اثبات حتی همین قضایای ساختاری محدود، باید از اطلاعات وسیعی در باب ساختار گروههای (بیش و کم) دلخواه استفاده کرد (بخشهای ۱، ۲، ۴، ۵، و ۸ از فصل ۱ و بخشهای ۴ و ۵ از فصل ۲). علاوه بر این، چند رده از گروههایی را مطالعه می‌کنیم که ساختار آنها در بخش وسیعی معلوم بوده و در سایر قسمتهای ریاضی کاربرد مفید دارند، از قبیل گروههای متقارن (بخش ۶)، گروههای آزاد [آبلی] (بخشهای ۹ و II ۱۰)، گروههای پوچ‌توان و حلپذیر (بخشهای II ۷۰ و II ۸۰).

یک نکتهٔ اساسی که نه تنها در مورد گروهها بلکه در مورد بسیاری از اشیاء جبری دیگر (مثلا"، حلقه‌ها، مدولها، فضاهای برداری، و میدانها) به کار می‌رود این است که در مطالعهٔ دقیق یک شیء با ساختاری جبری لازم است توابعی که این ساختار را حفظ می‌کنند (این نوع توابع را همریختی می‌نامند) نیز بررسی شوند. درواقع، چند مفهوم مشترک در نظریهٔ گروهها، حلقه‌ها، مدولها، و غیره را می‌توان برحسب اشیاء و همریختیها کاملا" توصیف کرد. در بخش ۷، جهت ساختن زبان مناسب و چارچوب ادراکی

مفید برای تصور این مفاهیم مشترک، واژهٔ رسته معرفی و پس از آن مکرر به کار گرفته شده است. البته، مطالعهٔ گروهها، حلقه‌ها، و غیره بدون حتی ذکر نام رسته امکان‌پذیر است. با اینحال، کمی زحمت برای درک این مفهوم در اینجا سود زیادی بعداً می‌دهد در این جهت که درک ما از روابط اساسی میان ساختارهای مختلف جبری که با آنها مواجه می‌شویم افزایش خواهد یافت.

بجز چند استثنا نظیر بخش ۷، هر بخش این فصل به بخشهای قبلی خود وابسته است.

۱ نیمگروهها، تکگونها، و گروهها

اگر G مجموعه‌ای ناتهی باشد، یک **عمل دوتایی** بر G تابعی است مانند $G \times G \to G$. برای نقش (a,b) تحت یک عمل دوتایی نمادهای مختلفی به‌کار می‌رود: ab (نماد ضربی)، $a+b$ (نماد جمعی)، $a \cdot b$، $a * b$، و غیره. برای راحتی، در سراسر این فصل عموماً از نماد ضربی استفاده می‌کنیم و ab را **حاصلضرب** a و b می‌نامیم. بر یک مجموعه ممکن است چند عمل دوتایی تعریف شده باشند (مثلاً، جمع و ضرب معمولی بر $\mathbf{Z}$ که به ترتیب با $(a,b) \mapsto a+b$ و $(a,b) \mapsto ab$ داده می‌شوند).

تعریف ۱.۱. یک **نیمگروه** عبارت است از مجموعه‌ای ناتهی مانند G همراه با عملی دوتایی بر G با خاصیت زیر:

(یک) شرکتپذیر: به‌ازای هر $a, b, c \in G$، $a(bc) = (ab)c$.

یک **تکگون** نیمگروهی است مانند G که شامل

(دو) یک عنصر همانی (دوطرفه) مانند $e \in G$ است به‌طوری‌که به‌ازای هر $a \in G$،

$ae = ea = a$.

یک **گروه** تکگونی است مانند G به‌طوری‌که

(سه) به‌ازای هر $a \in G$، عنصری معکوس (دوطرفه) مانند $a^{-1} \in G$ وجود دارد به قسمی که $a^{-1}a = aa^{-1} = e$. نیمگروه G را **آبلی** یا **تعویضپذیر** گویند اگر عمل دوتایی آن

(چهار) تعویضپذیر باشد: به‌ازای هر $a, b \in G$، $ab = ba$.

توجه اصلی ما به گروهها است. با اینحال برای بیان قضایا در منتهای کلیت، نیمگروهها

و تکگونها مناسب می‌باشند. مثالهایی ذیلا" آورده شده‌اند. مرتبهٔ گروه G عدد اصلی $|G|$ است. G را متناهی [نامتناهی] گویند اگر $|G|$ متناهی [نامتناهی] باشد.

قضیهٔ ۲.۱. *هرگاه G یک تکگون باشد، آنگاه عنصر همانی e منحصر به فرد است.*
هرگاه G یک گروه باشد، آنگاه
(یک) $c \in G$ و $cc = c \Rightarrow c = e$؛
(دو) *به‌ازای هر* $a, b, c \in G$، $ab = ac \Rightarrow b = c$ و $ba = ca \Rightarrow b = c$ *(حذف از چپ و راست)*؛
(سه) *به‌ازای هر* $a \in G$، *عنصر معکوس* a^{-1} *منحصر به فرد است*؛
(چهار) *به‌ازای هر* $a \in G$، $(a^{-1})^{-1} = a$؛
(پنج) *به‌ازای هر* $a, b \in G$، $(ab)^{-1} = b^{-1}a^{-1}$؛
(شش) *به‌ازای* $a, b \in G$، *معادلات* $ax = b$ و $ya = b$ *در* G *جوابهای منحصر به فرد* $x = a^{-1}b$ و $y = ba^{-1}$ *دارند*.

طرح برهان. هرگاه e' نیز یک همانی دوطرفه باشد، آنگاه $e = ee' = e'$. (یک)
$$ec = c \Rightarrow c^{-1}(cc) = c^{-1}c \Rightarrow (c^{-1}c)c = c^{-1}c \Rightarrow ec = e \Rightarrow c = e$$
(دو)، (سه)، و (شش) به همین نحو ثابت می‌شوند. (پنج) بنابر (سه)،
$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae)a^{-1} = aa^{-1} = e \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$$
(چهار) به همین نحو ثابت می‌شود.

هرگاه G تکگون بوده و عمل دوتایی آن به صورت ضرب نوشته شود، آنگاه عنصر همانی G همواره با e نموده می‌شود. هرگاه عمل دوتایی به‌صورت جمع نوشته شود، آنگاه $a + b$ $(a, b \in G)$ مجموع a و b نام دارد، و عنصر همانی با 0 نموده می‌شود: اگر G یک گروه باشد، معکوس $a \in G$ با $-a$ نموده می‌شود. برای $a + (-b)$ می‌نویسیم $a - b$. گروههای آبلی اغلب جمعی در نظر گرفته می‌شوند. اصول موضوع مذکور در تعریف ۱.۱ برای تعریف گروه را می‌توان به میزان قابل‌توجهی ضعیف کرد.

حکم ۳.۱. *فرض کنیم G یک نیمگروه باشد. G گروه است اگر و فقط اگر شرایط زیر برقرار*

باشند:

(یک) عنصری مانند $e \in G$ موجود باشد به‌طوری که به ازای هر $a \in G$ ، $ea = a$ (عنصر همانی چپ)؛

(دو) به‌ازای هر $a \in G$ ، عنصری مانند $a^{-1} \in G$ موجود باشد به‌طوری‌که $a^{-1}a = e$ (معکوس چپ).

تبصره. نتیجه‌ای مشابه برای "معکوسهای راست" و "همانی راست" برقرار است.

طرح برهان ۳.۱ ($\Leftarrow$) بدیهی است. ($\Rightarrow$) توجه کنید که قضیهٔ ۲.۱ (یک) تحت این مفروضات درست است. $G \neq \emptyset$ ، زیرا $e \in G$. هرگاه $a \in G$ ، آنگاه، طبق (دو)،

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = a(ea^{-1}) = aa^{-1}$$

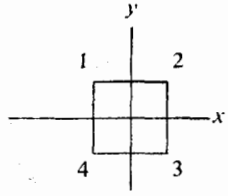
و در نتیجه، بنا بر قضیهٔ ۲.۱ (یک)، $aa^{-1} = e$. لذا، a^{-1} یک معکوس دوطرفهٔ a است. چون به‌ازای هر $a \in G$ ، $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ ، e یک همانی دوطرفه است. لذا، طبق تعریف ۱.۱ ، G گروه می‌باشد.

حکم ۴.۱. *فرض کنیم G یک نیمگروه باشد. G گروه است اگر و فقط اگر به ازای هر $a, b \in G$ ، معادلات $ax = b$ و $ya = b$ در G جواب داشته باشند.*

برهان. تمرین؛ از حکم ۳.۱ استفاده کنید.

چند مثال. اعداد صحیح $\mathbf{Z}$ ، اعداد گویای $\mathbf{Q}$ ، و اعداد حقیقی $\mathbf{R}$ تحت عمل جمع معمولی گروههای آبلی نامتناهی‌اند. هر یک از آنها تحت ضرب معمولی تگون است، ولی گروه نمی‌باشد (0 معکوس ندارد). اما عنصرهای ناصفر $\mathbf{Q}$ و $\mathbf{R}$ تحت ضرب گروه آبلی نامتناهی تشکیل می‌دهند. اعداد صحیح زوج تحت ضرب نیمگروهی است که تگون نمی‌باشد.

مثال. مربعی در نظر می‌گیریم که رئوسش اعداد 1,2,3,4 ، مرکزش در مبدأ صفحهٔ xy ، و اضلاعش موازی محورها باشند.



فرض کنیم D_4^* مجموعهٔ زیر از "تبدیلات" مربع باشد:

$$D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{1,3}, T_{2,4}\}$$

که در آن R دوران $90°$ حول مرکز در جهت خلاف عقربه‌های ساعت، R^2 دوران $180°$ در جهت خلاف عقربه‌های ساعت، R^3 دوران $270°$ در جهت خلاف عقربه‌های ساعت، و I دوران $360°$ $(= 0°)$ است؛ T_x انعکاس نسبت به محور x و $T_{1,3}$ انعکاس نسبت به قطر مار بر راسهای 1 و 3 است؛ و به همین ترتیب، T_y و $T_{2,4}$. توجه کنید که هر $U \in D_4^*$ یک بیژکسیون مربع به روی آن می‌باشد. عمل دوتایی در D_4^* را ترکیب توابع تعریف می‌کنیم: به‌ازای $U, V \in D_4^*$، $U \circ V$ تبدیل V و سپس تبدیل U می‌باشد. D_4^* یک گروه غیرآبلی از مرتبهٔ 8 است که **گروه تقارنهای مربع** نامیده می‌شود. توجه کنید که هر تقارن (عنصر D_4^*) کاملا" به وسیلهٔ عملش بر رئوس معین می‌شود.

مثال. فرض کنیم S یک مجموعهٔ ناتهی بوده و $A(S)$ مجموعهٔ تمام بیژکسیونهای $S \to S$ باشد. تحت عمل ترکیب توابع، یعنی $f \circ g$، $A(S)$ گروه است، زیرا ترکیب توابع شرکتپذیر است، ترکیب بیژکسیونها بیژکسیون است، 1_S بیژکسیون است، و هر بیژکسیون معکوس‌دارد (ر.ک. رابطهٔ (۱۳) آشنایی، بخش ۳). عنصرهای $A(S)$ **جایگشت** نام دارند و $A(S)$ گروه جایگشتها بر مجموعهٔ S نامیده‌می‌شود. هرگاه $S = \{1,2,3,\ldots,n\}$، آنگاه $A(S)$ **گروه متقارن بر n حرف** نام داشته و با S_n نموده می‌شود. تحقیق کنید که $|S_n| = n!$ (تمرین ۵). گروههای S_n نقش مهمی در نظریهٔ گروههای متناهی ایفا می‌کنند.

چون عنصر σ از S_n تابعی بر مجموعهٔ متناهی $S = \{1,2,\ldots,n\}$ است، می‌توان آن‌را با ذکر عناصر S بر یک خط و نقش هر عنصر تحت σ بلافاصله زیر آن توصیف کرد:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & & i_n \end{pmatrix}$$

. حاصلضرب $\sigma\tau$ دو عنصر S_n تابع ترکیب τ و پس‌از آن σ

می‌باشد؛ یعنی، تابعی است بر S که با $k \mapsto \sigma(\tau(k))$ داده می‌شود.[1] مثلاً"، فرض کنیم $\sigma = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ و $\tau = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$ عناصری از S_4 باشند. در این صورت، تحت $\sigma\tau$، $1 \mapsto \sigma(\tau(1)) = \sigma(4) = 4$، و از این قبیل؛ لذا،

$$\sigma\tau = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix};$$

به همین نحو،

$$\tau\sigma = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}.$$

این مثال نیز نشان می‌دهد که S_n لزوماً" آبلی نیست.

روش زیر، که از گروههای موجود گروههای جدید می‌سازد، ما را به منبع دیگری از مثالها هدایت می‌کند. G و H را گروههایی با همانیهای e_G, e_H می‌گیریم، و **حاصلضرب مستقیم** G و H را گروهی با مجموعهٔ زمینهٔ $G \times H$ و عمل دوتایی زیر تعریف می‌کنیم:

$$(a,b)(a',b') = (aa',bb')$$

که در آن $a,a' \in G; b,b' \in H$.

توجه کنید که در تعریف فوق سه عمل متفاوت در G، H، و $G \times H$ وجود دارند. به آسانی تحقیق می‌شود که $G \times H$، درواقع، گروه است و با فرض آبلی بودن G و H آبلی می‌شود؛ (e_G,e_H) همانی و (a^{-1},b^{-1}) معکوس (a,b) است. واضح است که $|G \times H| = |G||H|$ (آشنایی، تعریف ۳۰۸). هرگاه عمل G و H به صورت جمعی نوشته شود، آنگاه $G \oplus H$ را به جای $G \times H$ می‌نویسیم.

قضیهٔ ۵۰۱. *فرض کنیم* $\sim$ (R) *یک رابطهٔ هم‌ارزی بر تکگون* G *باشد به طوری که* $a_1 \sim a_2$ *و* $b_1 \sim b_2$ *ایجاب کنند که به‌ازای هر* $a_1,b_1 \in G$، $a_1b_1 \sim a_2b_2$. *در این صورت، مجموعهٔ* G/R *از تمام رده‌های هم‌ارزی* G *تحت* R *یک تکگون تحت عمل دوتایی تعریف شده با* $(\bar{a})(\bar{b}) = \overline{ab}$ *است، که در آن* $\bar{x}$ *ردهٔ هم‌ارزی* $x \in G$ *می‌باشد. هرگاه* G *یک گروه [آبلی] باشد، آنگاه* G/R *نیز چنین است.*

یک رابطهٔ هم ارزی بر تکگون G که در مفروضات قضیهٔ فوق صدق کند یک *رابطهٔ*

---

۱. در بسیاری از کتابها، حاصلضرب $\sigma\tau$ با "σ و پس از آن τ" تعریف می‌شود.

همنهشتی بر G نام دارد.

برهان ۵.۱ . هرگاه $\bar{a}_1 = \bar{a}_2$ و $\bar{b}_1 = \bar{b}_2$ $(a_i, b_i \in G)$ ، آنگاه ، طبق رابطهٔ (۲۰) درآشنایی، بخش ۴ ، $a_1 \sim a_2$ و $b_1 \sim b_2$. دراین‌صورت ، طبق‌فرض ، $a_1b_1 \sim a_2b_2$ ؛ درنتیجه ، مجدداً طبق (۲۰) ، $\overline{a_1b_1} = \overline{a_2b_2}$. لذا ، عمل دوتایی در G/R تعریف شده است (یعنی ، از انتخاب نماینده‌های ردهٔ هم‌ارزی مستقل است) . این رابطه شرکتپذیر است ، زیرا $\bar{e}.\ \bar{a}(\bar{b}\,\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{(ab)}\bar{c} = (\bar{a}\,\bar{b})\bar{c}$ عنصر همانی است ، زیرا $(\bar{a})(\bar{e}) = \overline{ae} = \bar{a} = \overline{ea} = (\bar{e})(\bar{a})$. بنابر این ، G/R تکگون است . هرگاه G گروه باشد ، آنگاه $\bar{a} \in G/R$ دارای معکوس $\overline{a^{-1}}$ است ؛ درنتیجه ، G/R نیز گروه است . به همین نحو ، آبلی بودن G آبلی بودن G/R را ایجاب می‌کند .

مثال . فرض‌کنیم m عدد صحیح ثابتی باشد . بنابر قضیهٔ ۸.۶ درآشنایی، همنهشتی به پیمانهٔ m یک‌رابطهٔ همنهشتی برگروه‌جمعی $\mathbf{Z}$ است . فرض‌کنیم Z_m مجموعهٔ رده‌های هم‌ارزی $\mathbf{Z}$ تحت همنهشتی به پیمانهٔ m باشد . بنابر قضیهٔ ۵.۱ (با نماد جمعی) Z_m با عمل جمع $(a,b \in \mathbf{Z})\ \bar{a} + \bar{b} = \overline{a+b}$ ، یک‌گروه‌آبلی‌است . برهان قضیهٔ ۸.۶ درآشنایی نشان می‌دهد که $Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ ؛درنتیجه ، Z_m ، تحت‌جمع ، یک گروه متناهی از مرتبهٔ m است . Z_m گروه (جمعی) **اعداد صحیح به پیمانهٔ m** نام دارد . به همین نحو ، چون $\mathbf{Z}$ تحت ضرب یک تکگون تعویضپذیر است ، و همنهشتی به پیمانهٔ m یک رابطهٔ همنهشتی نسبت به ضرب نیز هست (قضیهٔ ۸.۶ درآشنایی) ، Z_m با ضرب $(a,b \in \mathbf{Z})\ (\bar{a})(\bar{b}) = \overline{ab}$ یک تکگون تعویضپذیر است . تحقیق‌کنید که به‌ازای هر $\bar{a}, \bar{b}, \bar{c} \in Z_m$ ،

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{c} + \bar{b}\bar{c} \quad \text{و} \quad (\bar{a} + \bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$$ (پخشپذیری) .

به علاوه، هرگاه p اول باشد ، آنگاه عناصر ناصفر Z_p یک گروه ضربی از مرتبهٔ $p-1$ تشکیل می‌دهند (تمرین ۷) . رسم است که عناصر Z_m را به جای $\bar{0}, \bar{1}, \ldots, \overline{m-1}$ با $0, 1, \ldots, m-1$ نشان می‌دهند . این نماد مبهم مشکلی به بار نمی‌آورد و هر وقت مناسب بود به کار خواهد رفت .

مثال . رابطهٔ زیر برگروه‌جمعی $\mathbf{Q}$ از اعدادگویا یک رابطهٔ همنهشتی است (تمرین ۸) :

$$a \sim b \Leftrightarrow a - b \in \mathbf{Z}.$$

بنابر قضیهٔ ۵.۱ ، مجموعهٔ رده‌های هم‌ارزی (که با $\mathbf{Q/Z}$ نموده می‌شود) ، با جمع $\bar{a} + \bar{b} = \overline{a+b}$ ، یک گروه آبلی (نامتناهی) است. $\mathbf{Q/Z}$ **گروه اعداد گویا به پیمانهٔ یک** نام دارد.

فرض کنیم $a_1, \ldots, a_n \in G$ $(n \geq 3)$. شهودا " طرق موجه بسیاری برای درج پرانتز در عبارت $a_1 a_2 \cdots a_n$ برای به دست آوردن حاصل‌ضربی" با معنی " از این n عنصر با همین ترتیب در G وجود دارد. به علاوه، تساوی هر دو حاصل‌ضرب از این نوع را می‌توان با استفاده از قانون شرکتپذیری ثابت کرد. پیشنیاز لازم برای بررسی بیشتر گروهها و حلقه‌ها بیان و اثبات دقیق این حدسها و حدسهای مربوطه است.

به‌ازای هر دنباله‌ٔ $\{a_1, a_2 \ldots\}$ از عناصر نیمگروه G ، **حاصل‌ضرب با معنی** $a_1, \ldots, a_n$ (به همین ترتیب) را به استقرا تعریف می‌کنیم. اگر $n = 1$ ، تنها حاصل‌ضرب با معنی a_1 است. اگر $n > 1$ ، یک حاصل‌ضرب با معنی حاصل‌ضربی است که به شکل $(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ تعریف می‌شود، که در آن $m < n$ و $(a_1 \cdots a_m)$ و $(a_{m+1} \cdots a_n)$ به ترتیب حاصل‌ضربهای با معنی m و $n - m$ عنصراند.[1] توجه کنید که به‌ازای $n \geq 3$ ، ممکن است حاصل‌ضربهای با معنی بسیاری از $a_1, \ldots, a_n$ وجود داشته باشند. به‌ازای هر $n \in \mathbf{N}^*$ ، یک **حاصل‌ضرب** با معنی خاص **n عاملی متعارف** $\prod_{i=1}^{n} a_i$ از n عنصر $a_1, \ldots, a_n$ را می‌گزینیم و آن را به استقراچنین تعریف می‌کنیم :

$$\prod_{i=1}^{1} a_i = a_1 \quad ؛ \text{ و به‌ازای } n > 1 \text{ ،} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n \text{ .}$$

این امر که این تعریف به‌ازای هر $n \in \mathbf{N}^*$ معرف عنصر منحصر به فردی از G است (که به وضوح یک حاصل ضرب با معنی می‌باشد) از قضیهٔ ۲.۶ در آشنایی (تمرین ۱۶) نتیجه می‌شود.

قضیهٔ ۶.۱ (قانون شرکتپذیری تعمیم یافته). *هرگاه G یک نیمگروه بوده و $a_1, \ldots, a_n \in G$ ، آنگاه هر دو حاصل‌ضرب با معنی $a_1, \ldots, a_n$ با همین ترتیب مساوی‌اند.*

---

۱. *برای نشان دادن اعتبار این تعریف، به صورت دقیقتری از قضیهٔ بازگشتی ۲.۶ در آشنایی نیاز داریم، ر.ک. سی. دبلیو. بوریل* C. W. Burrill [۵۶؛ ص ۵۷] .

برهان. به استقرا نشان می‌دهیم که به‌ازای هر n ، هر حاصل ضرب با معنی از $a_1 \cdots a_n$ مساوی حاصل‌ضرب n عاملی متعارف $\prod_{i=1}^{n} a_i$ است. این به‌ازای $n = 1, 2$ به وضوح درست است. هرگاه $n > 2$ ، آنگاه، طبق تعریف، به‌ازای $m < n$ ی ، $(a_1 \cdots a_n) = (a_1 \cdots a_m)(a_{m+1} \cdots a_n)$. بنابراین، طبق استقرا و شرکتپذیری،

$$(a_1 \cdots a_n) = (a_1 \cdots a_m)(a_m \cdots a_n) = \left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m} a_{m+i}\right)$$
$$= \left(\prod_{i=1}^{m} a_i\right)\left(\left(\prod_{i=1}^{n-m-1} a_{m+i}\right)a_n\right) = \left(\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m-1} a_{m+i}\right)\right)a_n$$
$$= \left(\prod_{i=1}^{n-1} a_i\right)a_n = \prod_{i=1}^{n} a_i.$$

در پرتو قضیهٔ ۶۰۱ می‌توان هر حاصل‌ضرب با معنی از $a_1, \ldots, a_n \in G$ (G یک نیمگروه است) را بدون پرانتز و بی‌ابهام به صورت $a_1 a_2 \cdots a_n$ نوشت.

نتیجهٔ ۷۰۱ (قانون تعویضپذیری تعمیم یافته). هرگاه G یک نیمگروه تعویضپذیر بوده و $a_1, \ldots, a_n \in G$ ، آنگاه به‌ازای هر جایگشت $i_1, \ldots, i_n$ از $1, 2, \ldots n$ ، $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.

برهان. تمرین.

تعریف ۸۰۱. فرض‌کنیم G یک نیمگروه بوده، و $a \in G$ و $n \in \mathbf{N}^*$. عنصر $a^n \in G$ مساوی حاصل‌ضرب n عاملی متعارف $\prod_{i=1}^{n} a_i$ با $a_i = a$ به‌ازای $1 \leq i \leq n$ تعریف می‌شود. اگر G تکگون باشد، a^0 مساوی عنصر همانی e تعریف می‌شود. اگر G گروه باشد، به ازای هر $n \in \mathbf{N}^*$ ، a^{-n} مساوی $(a^{-1})^n \in G$ تعریف می‌گردد.

نکات پیش از قضیهٔ ۶۰۱ و تمرین ۱۶ نشان می‌دهند که نماگیری عملی تعریف شده است. در این صورت، طبق تعریف،

$$a^1 = a, a^2 = aa, a^3 = (aa)a = aaa, \ldots, a^n = a^{n-1}a = aa \cdots a \quad (n \text{ عامل})$$

توجه کنید که ممکن است به‌ازای $m \neq n$ ی داشته باشیم $a^m = a^n$ (مثلاً ، در C ،

$(-1 = i^2 = i^6$.

نماد جمعی . هرگاه عمل دوتایی در G را به صورت جمعی بنویسیم ، آنگاه به جای a^n می‌نویسیم na . مثلا " $0a = 0$ ، $1a = a$ ، $na = (n-1)a + a$ ، و از این قبیل .

قضیهٔ ۹.۱ . *هرگاه G گروه [نیمگروه یا تکگون] بوده و $a \in G$ ، آنگاه به‌ازای $m, n \in \mathbf{Z}$ [یا $\mathbf{N}^*$ یا $\mathbf{N}$] ،*

(یک) $a^m a^n = a^{m+n}$ *(با نماد جمعی :* $ma + na = (m+n)a$ *)؛*

(دو) $(a^m)^n = a^{mn}$ *(با نماد جمعی :* $n(ma) = mna$ *) .*

طرح برهان . تحقیق کنید که به‌ازای هر $n \in \mathbf{N}$ ، $(a^n)^{-1} = (a^{-1})^n$ و به‌ازای هر $n \in \mathbf{Z}$ ، $a^{-n} = (a^{-1})^n$. (یک) به‌ازای $m > 0$ و $n > 0$ درست است ، زیرا بنابر قضیهٔ ۶.۱ ، حاصلضرب یک حاصلضرب n عاملی متعارف و یک حاصلضرب m عاملی متعارف حاصلضربی با معنی و مساوی با حاصلضرب $(m+n)$ عاملی متعارف است . به‌ازای $m < 0$ و $n < 0$ ، a, m, n را با $a^{-1}, -m, -n$ تعویض‌کرده واستدلال قبلی را به کار برید. حالت $m = 0$ یا $n = 0$ بدیهی است و حالات $m \geq 0, n < 0$ و $m < 0, n \geq 0$ به‌ترتیب به استقرا بر m و n ثابت می‌شوند .

(دو) اگر $m = 0$ بدیهی‌است . حالتی که $m > 0$ و $n \in \mathbf{Z}$ به استقرا بر m ثابت می‌شود . با استفاده از این نتیجه ، حالت $m < 0$ و $n \in \mathbf{Z}$ را ثابت کنید .

تمرینات

۱ . مثالهایی از نیمگروه و تکگون غیر از مثالهای متن بزنید که گروه نباشند .

۲ . فرض کنید G یک گروه (به صورت جمعی) ، S مجموعه‌ای ناتهی ، و $M(S,G)$ مجموعهٔ تمام توابع $f : S \to G$ باشد . جمع در $M(S,G)$ را به صورت زیر تعریف می‌کنیم : $(f+g) : S \to G$ با $s \mapsto f(s) + g(s) \in G$ داده شده است . ثابت کنید $M(S,G)$ یک گروه است ، که در صورت آبلی بودن G آبلی می‌باشد .

۳ . آیا درست است که یک نیمگروه با عنصر همانی چپ که در آن هر عنصر معکوس راست دارد (ر.ک. حکم ۳.۱) گروه است ؟

۴ . برای گروه D_4^* جدول ضرب بنویسید .

۵ . ثابت کنید گروه متقارن بر n حرف ، یعنی S_n ، دارای مرتبهٔ $n!$ است .

۶ . برای $Z_2 \oplus Z_2$ جدول جمع بنویسید . $Z_2 \oplus Z_2$ را **گروه چهارگان کلاین** [1] می‌نامند .

۷ . هرگاه p اول باشد ، آنگاه عناصر نا صفر Z_p تحت ضرب یک گروه از مرتبهٔ $p-1$ تشکیل می‌دهند . [**راهنمایی** . $\bar{a} \neq \bar{0} \Rightarrow (a,p) = 1$ ؛ از قضیهٔ ۵.۶ در آشنایی استفاده کنید .] نشان دهید که این حکم در صورت اول نبودن p نادرست است .

۸ . (آ) رابطهٔ داده شده با $a \sim b \Leftrightarrow a - b \in \mathbf{Z}$ یک رابطهٔ همنهشتی بر گروه جمعی $\mathbf{Q}$ است [ر.ک. قضیهٔ ۵.۱] .

(ب) مجموعهٔ $\mathbf{Q/Z}$ از رده‌های هم‌ارزی یک گروه آبلی نامتناهی است .

۹ . فرض کنید p عدد اول ثابتی باشد . همچنین ، R_p مجموعهٔ تمام اعداد گویایی باشد که مخرجشان نسبت به p اول است . و نیز ، R^p مجموعهٔ اعداد گویایی باشد که مخرجشان توانی از p $(p^i,\ i \geq 0)$ باشد . ثابت کنید هر دوی R_p و R^p تحت جمع معمولی اعداد گویا گروههای آبلی‌اند .

۱۰ . فرض کنید p اول بوده و $Z(p^\infty)$ زیر مجموعهٔ زیر از گروه $\mathbf{Q/Z}$ باشد (ر.ک. ص ۴۲) :

$$Z(p^\infty) = \{\overline{a/b} \in \mathbf{Q/Z} \mid b = p^i \text{ ، ی } i \geq 0 \text{ و به‌ازای } a,b \in \mathbf{Z}\}.$$

نشان دهید که $Z(p^\infty)$ تحت عمل جمع $\mathbf{Q/Z}$ گروهی نامتناهی است .

۱۱ . شرایط زیر بر گروه G معادلند : (یک) G آبلی است ؛

(دو) به‌ازای هر $a,b \in G$ ، $(ab)^2 = a^2b^2$ ؛ (سه) به‌ازای هر $a,b \in G$ ، $(ab)^{-1} = a^{-1}b^{-1}$ ؛ (چهار) به‌ازای هر $n \in \mathbf{Z}$ و هر $a,b \in G$ ، $(ab)^n = a^nb^n$ ؛ (پنج) به‌ازای سه عدد صحیح متوالی n و هر $a,b \in G$ ، $(ab)^n = a^nb^n$ ، نشان دهید (یک) $\Leftrightarrow$ (پنج) درصورتی که "سه" با "دو" تعویض شود نادرست است.

۱۲ . هرگاه G گروه ، $a,b \in G$ ، وبه‌ازای $r \in \mathbf{N}$ ی ، $bab^{-1} = a^r$ ، آنگاه به‌ازای هر $j \in \mathbf{N}$ ، $b^jab^{-j} = a^{r^j}$.

۱۳ . هرگاه به‌ازای جمیع عناصر a از گروه G ، $a^2 = e$ ، آنگاه G آبلی است .

۱۴ . هرگاه G گروهی متناهی از مرتبهٔ زوج باشد ، آنگاه G شامل عنصری مانند $a \neq e$

---

1. **Klein**

است به‌طوری‌که $a^2 = e$.

۱۵ . فرض کنید G مجموعه‌ای متناهی و ناتهی با عمل دوتایی شرکتپذیری باشد به‌طوری‌که به‌ازای هر $a,b,c \in G$ ، $ab = ac \Rightarrow b = c$ و $ba = ca \Rightarrow b = c$. در این صورت ، G یک گروه است . نشان دهید که این امر در صورت نامتناهی بودن G ممکن است درست نباشد .

۱۶ . فرض کنید $a_1,a_2,\ldots$ دنباله‌ای از عناصر در نیمگروه G باشد . در این‌صورت ، تابع منحصربه‌فردی مانند $\psi : \mathbf{N}^* \to G$ هست به‌طوری که $\psi(1) = a_1$ ، $\psi(2) = a_1a_2$ ، $\psi(3) =$ ، $(a_1a_2)a_3$ و به‌ازای $n \geq 1$ ، $\psi(n+1) = (\psi(n))a_{n+1}$. توجه کنید که $\psi(n)$ دقیقاً حاصل‌ضرب n عاملی متعارف $\prod_{i=1}^{n} a_i$ است . [**راهنمایی .** با اعمال قضیهٔ بازگشتی ۲.۶ در آشنایی‌به‌ازای $a = a_1$ ، $S = G$ ، و $f_n : G \to G$ که با $x \mapsto xa_{n+2}$ داده شده است ، تابعی مانند $\varphi : \mathbf{N} \to G$ به دست می‌آید . فرض‌کنید $\psi = \varphi\theta$ ، که در آن $\theta : \mathbf{N}^* \to \mathbf{N}$ با $k \mapsto k - 1$ داده می‌شود .]

۲ همریختیها و زیرگروهها

در بررسی هر رده از اشیاء جبری ، توابعی که ساختار جبری را به معنی زیر حفظ می‌کنند از ضروریات می‌باشند .

تعریف ۱.۲ . فرض کنیم G و H نیمگروه باشند . تابع $f : G \to H$ یک **همریختی** است مشروط بر اینکه

به ازای هر $a,b \in G$ ، $f(ab) = f(a)f(b)$.

اگر f به عنوان نگاشتی از مجموعه‌ها انژکتیو باشد ، f یک **تکریختی** گفته می‌شود . اگر f سورژکتیو باشد ، f یک **برورریختی** نامیده می‌شود . چنانچه f بیژکتیو باشد ، f یک **یکریختی** نام دارد . در این حالت گویند G و H **یکریخت**‌اند (نوشته می‌شود $G \cong H$) . همریختی $f : G \to G$ یک **درونریختی** G و یکریختی $f : G \to G$ یک **خودریختی** G نامیده می‌شود .

اگر $f : G \to H$ و $g : H \to K$ همریختیهایی از نیمگروهها باشند ، به آسانی دیده می‌شود که $gf : G \to K$ نیز یک همریختی است . به همین نحو ، ترکیب تکریختیها یک

تکریختی است ؛ همچنین است برای برووریختیها ، یکریختیها ، و خودریختیها . هرگاه G و H گروههایی به‌ترتیب با همانیهای e_G و e_H بوده و $f: G \to H$ یک همریختی باشد ، آنگاه $f(e_G) = e_H$ ؛ اما این امر برای تکگونها درست نیست (تمرین ۱).به علاوه، به‌ازای هر $a \in G$ ، $f(a^{-1}) = f(a)^{-1}$ (تمرین ۱) .

مثال . نگاشت $f: \mathbf{Z} \to Z_m$ داده‌شده با $x \mapsto \bar{x}$ (یعنی ،هر عدد صحیح به رده‌ٔ هم‌ارزی خود در Z_m نگاشته شده‌است) یک برووریختی گروههای جمعی است . f برووریختی کانونی از $\mathbf{Z}$ به روی Z_m نامیده می‌شود.به همین نحو ، نگاشت $g: \mathbf{Q} \to \mathbf{Q/Z}$ داده شده با $r \mapsto \bar{r}$ نیز یک برووریختی گروههای جمعی است .

مثال . هرگاه A یک‌گروه آبلی باشد ، آنگاه نگاشت داده شده با $a \mapsto a^{-1}$ یک خودریختی A است . نگاشت داده شده با $a \mapsto a^2$ یک درونریختی A می‌باشد .

مثال . فرض کنیم $1 < m, k \in \mathbf{N}^*$. نگاشت $g: Z_m \to Z_{mk}$ داده شده با $x \mapsto \overline{kx}$ یک تکریختی است .

مثال . به‌ازای گروههای G و H ، چهار همریختی وجود دارند : $G \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} G \times H \underset{\pi_2}{\overset{\iota_2}{\leftrightarrows}} H$ که با $\iota_1(g) = (g,e)$; $\iota_2(h) = (e,h)$; $\pi_1(g,h) = g$; $\pi_2(g,h) = h$ داده می‌شوند . ι_i یک تکریختی است و π_i یک برووریختی می‌باشد $(i,j = 1,2)$.

تعریف ۲۰۲ . فرض کنیم $f: G \to H$ یک همریختی گروهها باشد . **هستهٔ** f (با $Ker\, f$ نموده می‌شود) عبارت است از $\{a \in G \mid f(a) = e \in H\}$. هرگاه A زیر مجموعه‌ای از G باشد ، آنگاه $\{b \in H \mid b = f(a)$ ای $a \in A\}$ به‌ازای $f(A)$ نقش A می‌باشد . $f(G)$ نقش f نامیده و با $Im\, f$ نموده می‌شود . اگر B زیرمجموعه‌ای از H باشد ، $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$ نقش معکوس B می‌باشد .

قضیهٔ ۳۰۲ . *فرض کنیم $f: G \to H$ یک همریختی گروهها باشد . در این صورت ،*
(یک) f یک تکریختی است اگر و فقط اگر $Ker\, f = \{e\}$ ؛

(دو) f **یک یکریختی است اگر و فقط اگر یک همریختی مانند** $f^{-1}: H \to G$ **وجود داشته باشد به طوری که** $ff^{-1} = 1_H$ و $f^{-1}f = 1_G$.

برهان (یک) . هرگاه f یک تکریختی بوده و $a \in \operatorname{Ker} f$ ، آنگاه $f(a) = e_H = f(e)$ ، که از آنجا $a = e$ و $\operatorname{Ker} f = \{e\}$. هرگاه $\operatorname{Ker} f = \{e\}$ و $f(a) = f(b)$ ، آنگاه $ab^{-1} = e$ ؛ درنتیجه ، $ab^{-1} \in \operatorname{Ker} f$. بنابراین ، $e_H = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ (یعنی ، $a = b$) و f یک تکریختی است .

(دو) هرگاه f یک یکریختی باشد ، آنگاه بنابر رابطهٔ (۱۳) درآشنایی، بخش ۳ ، نگاشتی از مجموعه‌ها مانند $f^{-1}: H \to G$ وجود دارد به‌طوری‌که $f^{-1}f = 1_G$ و $ff^{-1} = 1_H$. به آسانی دیده می‌شود که f^{-1} یک همریختی است . عکس مطلب نتیجهٔ فوری رابطهٔ (۱۳) درآشنایی، بخش ۳ ، و تعریف ۱.۲ است .

فرض کنیم G یک نیمگروه بوده و H زیرمجموعه‌ای ناتهی از G باشد . اگر به ازای هر $a,b \in H$ داشته باشیم $ab \in H$ ، گوییم H تحت ضرب در G **بسته** است . این معادل آن است که بگوییم عمل دوتایی بر G ، وقتی به H محدود شود ، یک عمل دوتایی بر H است .

تعریف ۴.۲ . فرض کنیم G یک گروه و H زیرمجموعه‌ای ناتهی از آن باشد که تحت ضرب در G بسته است . هرگاه H خود تحت عمل ضرب در G گروه باشد ، آنگاه گویند H یک **زیرگروه** G است . این امر با $H < G$ نموده می‌شود .

دو نمونه از زیرگروههای گروه G عبارتند از خود G و **زیرگروه بدیهی** $\langle e \rangle$ مرکب از فقط عنصر همانی . زیرگروه H با خاصیت $H \neq G, H \neq \langle e \rangle$ یک **زیرگروه حقیقی** نامیده می‌شود .

مثال . مجموعهٔ تمام مضارب عدد صحیح ثابت n یک زیرگروه $\mathbf{Z}$ است ، که با $\mathbf{Z}$ یکریخت است (تمرین ۷) .

مثال. در S_n ، یعنی گروه تمام جایگشتهای $\{1,2,\ldots,n\}$ ، مجموعهٔ تمام جایگشتهایی که n را ثابت می‌گذارند زیرگروهی یکریخت با S_{n-1} تشکیل می‌دهند (تمرین ۸).

مثال. در $Z_6 = \{0,1,2,3,4,5\}$ ، $\{0,3\}$ و $\{0,2,4\}$ هر دو تحت جمع زیرگروه می‌باشند. اگر p اول باشد، $(Z_p,+)$ زیرگروه حقیقی ندارد.

مثال. هرگاه $f: G \to H$ یک همریختی گروهها باشد، آنگاه $\operatorname{Ker} f$ زیرگروهی از G است. اگر A زیرگروهی از G باشد، $f(A)$ زیرگروهی از H است؛ بویژه، $\operatorname{Im} f$ زیرگروهی از H می‌باشد. اگر B زیرگروهی از H باشد، $f^{-1}(B)$ زیرگروهی از G است (تمرین ۹).

مثال. هرگاه G گروه باشد، آنگاه مجموعهٔ $\operatorname{Aut} G$ مرکب از تمام خودریختیهای G با عمل دوتایی ترکیب توابع یک گروه است (تمرین ۱۵).

بنابر قضیهٔ ۲۰۱، عنصر همانی هرزیرگروه H عنصر همانی G است و معکوس $a \in H$ معکوس a^{-1} از a در G می‌باشد.

قضیهٔ ۵۰۲. *فرض کنیم H زیرمجموعه‌ای ناتهی از گروه G باشد. H زیرگروهی از G است اگر و فقط اگر به‌ازای هر* $a,b \in H$ ، $ab^{-1} \in H$.

برهان ($\Rightarrow$). $a \in H$ ای وجود دارد؛ و درنتیجه، $e = aa^{-1} \in H$. لذا، به‌ازای هر $b \in H$ ، $b^{-1} = eb^{-1} \in H$. هرگاه $a,b \in H$، آنگاه $b^{-1} \in H$؛ ودرنتیجه $ab = a(b^{-1})^{-1} \in H$. ضرب در H شرکتپذیر است، زیرا G گروه می‌باشد. بنابراین، H یک (زیر)گروه است. عکس مطلب بدیهی است.

نتیجهٔ ۶۰۲. *هرگاه G یک گروه و* $\{H_i \mid i \in I\}$ *خانواده‌ای ناتهی از زیرگروهها باشد، آنگاه* $\bigcap_{i \in I} H_i$ *زیرگروهی از G است.*

برهان. تمرین.

تعریف ۷.۲ . فرض کنیم G یک گروه و X زیرمجموعه‌ای از G باشد . همچنین ، فرض کنیم $\{H_i \mid i \in I\}$ خانواده‌ٔ تمام زیرگروههای G باشد که شامل X اند . در این صورت ، $\bigcap_{i\in I} H_i$ **زیرگروه** G **تولید شده به وسیلهٔ مجموعهٔ** X نامیده و با $\langle X\rangle$ نموده می‌شود .

عناصر X ***مولدهای*** زیرگروه $\langle X\rangle$ اند ،که‌می‌توانند بازیرمجموعه‌های دیگرنیزتولیدشود (یعنی ، ممکن است داشته باشیم $\langle X\rangle = \langle Y\rangle$ با $X \neq Y$) . اگر $X = \{a_1, \ldots, a_n\}$ ، به جای $\langle X\rangle$ می‌نویسیم $\langle a_1, \ldots, a_n\rangle$. اگر $G = \langle a_1, \ldots, a_n\rangle, (a_i \in G)$ ، گویند G ***با تولید متناهی است*** . اگر $a \in G$ ، زیرگروه $\langle a\rangle$ را ***(زیر)گروه دوری*** تولید شده به وسیلهٔ a می‌نامند .

قضیهٔ ۸.۲ . ***هرگاه*** G ***یک گروه و*** X ***زیرمجموعه‌ای ناتهی از*** G ***باشد ، آنگاه زیرگروه*** $\langle X\rangle$ ***تولید شده به وسیلهٔ*** X ***مرکب است از تمام حاصل ضربهای متناهی*** $a_1^{n_1}a_2^{n_2}\ldots a_t^{n_t}$ $(a_i \in X; n_i \in Z)$. ***بخصوص ، به‌ازای هر*** $a \in G$ ، $\langle a\rangle = \{a^n \mid n \in Z\}$.

طرح برهان . نشان دهید که مجموعهٔ H مرکب از تمام این حاصلضربها یک زیرگروه G است که شامل X بوده و مشمول هرزیرگروه شامل X می‌باشد . بنابراین ، $H < \langle X\rangle < H$.

چند مثال . گروه جمعی $\mathbf{Z}$ یک گروه دوری نامتناهی با مولد 1است ، زیرا طبق تعریف ۸.۱ (نماد جمعی) ، به‌ازای هر $m \in \mathbf{Z}$ ، $m1 = m$. البته ، ***"توانهای" عنصر مولد،همانند در*** $\mathbf{Z}$***، لازم نیست همه متمایز باشند*** . زیرگروه بدیهی $\langle e\rangle$ از هر گروه دوری است ؛ زیرگروه ضربی $\langle i\rangle$ در $\mathbf{C}$ دوری از مرتبهٔ 4 است و ، به‌ازای هر m ، گروه جمعی Z_m دوری از مرتبهٔ m با مولد $1 \in Z_m$ می‌باشد . در بخش ۳ ثابت خواهیم کرد که هر زیرگروه دوری با $\mathbf{Z}$ یا Z_m ، به‌ازای m ی ، یکریخت است . همچنین ، ر.ک. تمرین ۱۲ .

هرگاه $\{H_i \mid i \in I\}$ خانواده‌ای از زیرگروههای گروه G باشد ، آنگاه $\bigcup_{i\in I} H_i$ در حالت کلی زیرگروه G نیست . زیرگروه $\langle \bigcup_{i\in I} H_i\rangle$ تولید شده به وسیلهٔ مجموعهٔ $\bigcup_{i\in I} H_i$ **زیرگروه تولید شده به وسیلهٔ** ***گروههای*** $\{H_i \mid i \in I\}$ نامیده می‌شود . اگر H و K زیرگروه باشند ، زیرگروه $\langle H \cup K\rangle$ تولید شده به وسیلهٔ H و K ***الحاق*** H و K نامیده و با $H \vee K$ نموده

می‌شود (نماد جمعی : $H + K$) .

تمرینات

۱ . هرگاه $f: G \to H$ یک‌همریختی گروهها باشد ، آنگاه $f(e_G) = e_H$ و به‌ازای هر $a \in G$ ، $f(a^{-1}) = f(a)^{-1}$. با مثال نشان دهید که اگر تکگونهای G, H گروه نباشند ، نتیجهٔ اول ممکن است درست نباشد .

۲ . گروه G آبلی است اگر و فقط اگر نگاشت $G \to G$ داده شده با $x \mapsto x^{-1}$ یک خودریختی باشد .

۳ . فرض کنید Q_8 گروه (تحت ضرب ماتریس معمولی) تولید شده به وسیلهٔ ماتریسهای مختلط $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ و $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ باشد ، که $i^2 = -1$. نشان دهید که Q_8 یک‌گروه غیرآبلی از مرتبهٔ 8 است . Q_8 **گروه چهارتایی** نامیده می‌شود . [**راهنمایی** . توجه کنید که $BA = A^3B$ ؛ در نتیجه ، هر عنصر Q_8 به صورت A^iB^j می‌باشد . همچنین ، توجه داشته باشید که $A^4 = B^4 = I$ ، که در آن $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ عنصر همانی Q_8 است .]

۴ . فرض کنید H گروه (تحت ضرب ماتریسی) ماتریسهای حقیقی تولید شده به وسیلهٔ $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ و $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ باشد . نشان دهید که H یک‌گروه غیرآبلی از مرتبهٔ 8 است که با گروه چهارتایی تمرین ۳ یکریخت نیست ، ولی با گروه D_4^* یکریخت است .

۵ . فرض کنید S یک‌زیرمجموعهٔ ناتهی از گروه G بوده ، و رابطه‌ای بر G را با $a \sim b$ تعریف می‌کنیم اگر و فقط اگر $ab^{-1} \in S$. نشان دهید که $\sim$ یک رابطهٔ هم‌ارزی است اگر و فقط اگر S زیر گروه G باشد .

۶ . یک زیرمجموعه متناهی ناتهی گروه G زیرگروه است اگر و فقط اگر تحت ضرب در G بسته باشد .

۷ . هرگاه n عددصحیح ثابتی باشد ، آنگاه $\{kn \mid k \in \mathbf{Z}\} \subset \mathbf{Z}$ یک‌زیرگروه‌جمعی $\mathbf{Z}$ است ، که با $\mathbf{Z}$ یکریخت می‌باشد .

۸ . مجموعهٔ $\{\sigma \in S_n \mid \sigma(n) = n\}$ یک زیرگروه S_n است که با S_{n-1} یکریخت است .

۹ . فرض کنید $f: G \to H$ یک همریختی گروهها بوده ، A زیرگروهی از G و B زیرگروهی از H باشد .

(آ) $\operatorname{Ker} f$ و $f^{-1}(B)$ زیرگروههایی از G اند .

(ب) $f(A)$ زیرگروهی از H است .

۱۰ . تمام زیرگروههای $Z_2 \oplus Z_2$ را ذکر کنید . آیا $Z_2 \oplus Z_2$ با Z_4 یکریخت است ؟

۱۱ . هرگاه G گروه باشد ، آنگاه $C = \{a \in G \mid ax = xa \ ، \ x \in G\}$ به‌ازای هر یک زیرگروه آبلی از G است . C مرکز G نامیده می‌شود .

۱۲ . گروه D_4* دوری نیست ، اما می‌تواند با دو عنصر تولید شود . همین امر برای S_n درست است (نابدیهی) . تعداد مینیمال مولدهای گروه جمعی $\mathbf{Z} \oplus \mathbf{Z}$ چند است ؟

۱۳ . هرگاه $G = \langle a \rangle$ یک گروه دوری و H یک گروه باشد ، آنگاه هر همریختی $f: G \to H$ کاملا" به وسیلهٔ عنصر $f(a) \in H$ معین می‌شود .

۱۴ . زیرگروههای دوری زیر همه یکریخت‌اند : گروه ضربی $\langle i \rangle$ در $\mathbf{C}$ ، گروه جمعی Z_4 ، و زیرگروه $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ از S_4 .

۱۵ . فرض کنید G یک گروه و $\operatorname{Aut} G$ مجموعهٔ تمام خود ریختیهای G باشد .

(آ) $\operatorname{Aut} G$ با ترکیب توابع به عنوان عمل دوتایی گروه است .

[**راهنمایی** . $1_G \in \operatorname{Aut} G$ همانی است ؛ معکوسها طبق قضیهٔ ۳۰۲ وجود دارند .]

(ب) $\operatorname{Aut} \mathbf{Z} \cong Z_2$ و $\operatorname{Aut} Z_6 \cong Z_2$ ؛ $\operatorname{Aut} Z_8 \cong Z_2 \oplus Z_2$ ؛ $\operatorname{Aut} Z_p \cong Z_{p-1}$ (p اول) .

(پ) $\operatorname{Aut} Z_n$ به‌ازای $n \in \mathbf{N}^*$ دلخواه چیست ؟

۱۶ . به‌ازای هر p اول ، زیرگروه جمعی $Z(p^\infty)$ از $\mathbf{Q}/\mathbf{Z}$ (تمرین ۱۰۰۱) به وسیلهٔ مجموعهٔ $\{1/p^n \mid n \in \mathbf{N}^*\}$ تولید شده است .

۱۷ . فرض کنید G یک گروه آبلی و H, K زیرگروههای G باشند . نشان دهید که الحاق $H \vee K$ مجموعهٔ $\{ab \mid a \in H, b \in K\}$ است . این نتیجه را به هر تعداد متناهی از زیرگروههای G تعمیم دهید .

۱۸ . (آ) فرض کنید G یک گروه و $\{H_i \mid i \in I\}$ خانواده‌ای از زیرگروهها باشد . شرطی را بیان و ثابت کنید که زیر گروه بودن $\bigcup_{i \in I} H_i$ را ایجاب کند ؛ یعنی $\bigcup_{i \in I} H_i = \langle \bigcup_{i \in I} H_i \rangle$.

(ب) گروه G و خانوادهٔ $\{H_i \mid i \in I\}$ از زیرگروهها را چنان مثال بزنید که $\bigcup_{i\in I} H_i \neq \langle \bigcup_{i\in I} H_i \rangle$.

۱۹. (آ) مجموعهٔ تمام زیرگروههای گروه G، که به وسیلهٔ شمول نظریهٔ مجموعه‌ها جزئی مرتب شده است، یک شبکهٔ تام تشکیل می‌دهد (آشنایی،تمرینات ۱۰۷ و ۲۰۷) که در آن g.l.b مجموعهٔ $\{H_i \mid i \in I\}$ مساوی $\bigcap_{i\in I} H_i$ است و l.u.b آن برابر $\langle \bigcup_{i\in I} H_i \rangle$.

(ب) شبکهٔ زیرگروههای گروههای S_3, D_4^*, Z_6, Z_{27}، و Z_{36} را نشان دهید.

۳ گروههای دوری

ساختار گروههای دوری نسبتاً ساده است. ما همهٔ گروههای دوری را کاملاً (با تقریب یکریختی) مشخص خواهیم کرد.

قضیهٔ ۱۰۳. *هر زیرگروه H از گروه جمعی $\mathbf{Z}$ دوری است. یا $H = \langle 0 \rangle$ یا $H = \langle m \rangle$، که در آن m کوچکترین عدد صحیح مثبت در H است. هرگاه $H \neq \langle 0 \rangle$، آنگاه H نامتناهی است.*

برهان. $H = \langle 0 \rangle$ یا H شامل کوچکترین عدد صحیح مثبت m است. واضح است که $\langle m \rangle = \{km \mid k \in \mathbf{Z}\} \subset H$. به عکس، هرگاه $h \in H$، آنگاه $h = qm + r$ با $q, r \in \mathbf{Z}$ و $0 \leq r < m$ (الگوریتم تقسیم). چون $r = h - qm \in H$، مینیمالی m ایجاب می‌کند که $r = 0$ و $h = qm$. از اینرو، $H \subset \langle m \rangle$. اگر $H \neq \langle 0 \rangle$، واضح است که $H = \langle m \rangle$ نامتناهی است.

قضیهٔ ۲۰۳. *هر گروه دوری نامتناهی با گروه جمعی $\mathbf{Z}$ یکریخت است و هر گروه دوری متناهی از مرتبهٔ m با گروه جمعی Z_m یکریخت می‌باشد.*

برهان. هرگاه $G = \langle a \rangle$ یک گروه دوری باشد، آنگاه، بنابر قضایای ۹۰۱ و ۸۰۲، نگاشت $\alpha : \mathbf{Z} \to G$ داده شده با $k \mapsto a^k$ یک بروریختی است. هرگاه $\operatorname{Ker} \alpha = 0$، آنگاه، بنابر قضیهٔ ۳۰۲ (یک)، $\mathbf{Z} \cong G$. درغیر اینصورت، $\operatorname{Ker} \alpha$ یک زیرگروه نابدیهی $\mathbf{Z}$ است (تمرین ۹۰۲)؛ و درنتیجه، $\operatorname{Ker} \alpha = \langle m \rangle$، که در آن m کوچکترین عدد صحیح مثبتی است

که $a^m = e$ (قضیهٔ ۱۰۳) . به‌ازای هر $r, s \in \mathbf{Z}$ ،

$$a^r = a^s \iff a^{r-s} = e \iff r - s \in \operatorname{Ker} \alpha = \langle m \rangle$$
$$\iff m \mid (r - s) \iff Z_m \text{ در } \bar{r} = \bar{s},$$

(در آن $\bar{k}$ ردهٔ همنهشتی $k \in \mathbf{Z}$ است) . بنابراین ، نگاشت $\beta : Z_m \to G$ داده شده با $\bar{k} \mapsto a^k$ یک برورِیختی تعریف شده است . چون

$$\beta(\bar{k}) = e \iff a^k = e = a^0 \iff Z_m \text{ در } \bar{k} = \bar{0},$$

β یک تکریختی است (قضیهٔ ۳۰۲ (یک)) ؛ و در نتیجه ، یک یکریختی $Z_m \cong G$.

تعریف ۳۰۳ . فرض کنیم G یک گروه بوده و $a \in G$. **مرتبهٔ** a زیرگروه دوری $\langle a \rangle$ است و با $|a|$ نموده می‌شود .

قضیهٔ ۴۰۳ . فرض کنیم G یک گروه بوده و $a \in G$. **هرگاه** a **مرتبهٔ نامتناهی داشته باشد ، آنگاه**

(یک) $a^k = e$ **اگر و فقط اگر** $k = 0$ ؛

(دو) عناصر a^k $(k \in \mathbf{Z})$ **همه متمایزند ؛**

هرگاه a **مرتبهٔ متناهی** $m > 0$ **داشته باشد ، آنگاه**

(سه) m **کوچکترین عدد صحیح مثبتی است که** $a^m = e$ ؛

(چهار) $a^k = e$ **اگر و فقط اگر** $m \mid k$ ؛

(پنج) $a^r = a^s$ اگر و فقط اگر $r \equiv s \pmod{m}$ ؛

(شش) $\langle a \rangle$ **مرکب از عناصر متمایز** $a, a^2, \ldots, a^{m-1}, a^m = e$ **است ؛**

(هفت) به ازای هر k **که** $k \mid m$ **، داریم** $|a^k| = m/k$

طرح برهان . قسمتهای (یک) تا (شش) نتایج فوری برهان قضیهٔ ۲۰۳ هستند .
(هفت) $(a^k)^{m/k} = a^m = e$ و به ازای هر $0 < r < m/k$ ، $(a^k)^r \neq e$ ، زیرا در غیر این صورت ، $a^{kr} = e$ با خاصیت $kr < k(m/k) = m$ ، که با (سه) متناقض است . بنابراین ، طبق (سه) ، $|a^k| = m/k$.

قضیهٔ ۵۰۳ . هر نقش همریختی و هر زیرگروه یک گروه دوری G دوری است . بخصوص ،

هرگاه H یک زیرگروه نابدیهی $G = \langle a \rangle$ بوده و m کوچکترین عدد صحیح مثبتی باشد که $a^m \in H$، آنگاه $H = \langle a^m \rangle$.

طرح برهان. هرگاه $f: G \to K$ یک همریختی گروهها باشد، آنگاه $\operatorname{Im} f = \langle f(a) \rangle$. برای اثبات حکم دوم کافی است برهان قضیهٔ ۱.۳ را به نماد ضربی ترجمه کنیم (یعنی، در سراسر برهان هر $t \in \mathbf{Z}$ را با a^t عوض کنیم). این برهان حتی اگر G متناهی باشد کاراست.

یادآور می‌شویم که دو عنصر متمایز در یک گروه ممکن است یک زیرگروه دوری تولید کنند.

قضیهٔ ۶.۳. فرض کنیم $G = \langle a \rangle$ گروهی دوری باشد. هرگاه G نامتناهی باشد، آنگاه a و a^{-1} تنها مولدهای G اند. هرگاه G متناهی از مرتبهٔ m باشد، آنگاه a^k یک مولد G است اگر و فقط اگر $(k,m) = 1$.

طرح برهان. کافی است فرض کنیم $G = \mathbf{Z}$، که در این حالت اثبات آسان است، یا اینکه $G = Z_m$. اگر $(k,m) = 1$، عنصرهایی مانند $c,d \in \mathbf{Z}$ وجود دارند به‌طوری‌که $ck + dm = 1$؛ با استفاده از این، نشان دهید که $\bar{k}$، Z_m را تولید می‌کند. اگر $(k,m) = r > 1$، نشان دهید. که به‌ازای $n = m/r < m$، $n\bar{k} = \overline{nk} = 0$؛ ودرنتیجه، $\bar{k}$ نمی‌تواند Z_m را تولیدکند.

طبعا" این امید هست که تکنیکهای به کار رفته در بالا را می‌توان به گروهها با دو مولد و مآلا" به تمام گروههای با تولید متناهی تعمیم داد؛ و لذا، توصیفی از ساختار این گروهها فراهم آورد. اما، متاسفانه، حتی گروهها با فقط دو مولد ممکن است ساختار بسیار پیچیده‌ای داشته باشند. (مثلا"، ممکن است آبلی نباشند؛ ر.ک. تمرینات ۳.۲، و ۴.۲.) مآلا" خواهیم توانست تمام گروههای آبلی با تولید متناهی را مشخص نماییم، اما حتی این نیز به کار ماشینی زیادی نیاز دارد.

تمرینات

۱. فرض کنید a,b عنصرهایی از گروه G باشند. نشان دهید که $|a| = |a^{-1}|$؛

$|ab| = |ba|$ ؛ و به ازای هر $c \in G$ ، $|a| = |cac^{-1}|$.

۲ . فرض کنید گروه آبلی G شامل عناصر a و b به ترتیب از مراتب m و n باشد. نشان دهید G شامل عنصری است که مرتبه‌اش کوچکترین مضرب مشترک m و n است. [**راهنمایی** . ابتدا حالت $(m,n) = 1$ را حل کنید .]

۳ . فرض کنید G گروهی آبلی از مرتبهٔ pq ، با $(p,q) = 1$ ، باشد. همچنین ، $a,b \in G$ ای موجود باشند به‌طوری‌که $|a| = p, |b| = q$. نشان دهید G دوری است.

۴ . هرگاه $f: G \to H$ یک همریختی باشد ، $a \in G$ ، و $f(a)$ دارای مرتبهٔ متناهی در H باشد، آنگاه $|a|$ نامتناهی‌است یا $|f(a)|$ ، $|a|$ را عاد می‌کند.

۵ . فرض کنید G گروه ضربی تمام ماتریسهای 2×2 نامنفرد با درایه‌های گویا باشد. نشان دهید $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ دارای مرتبهٔ 4 و $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ دارای مرتبهٔ 3 است ، ولی ab دارای مرتبهٔ نامتناهی می‌باشد. به عکس، نشان دهید که گروه جمعی $Z_2 \oplus \mathbf{Z}$ شامل عناصر ناصفر a,b از مرتبهٔ نامتناهی است به‌طوری که $a+b$ مرتبهٔ متناهی دارد.

۶ . هرگاه G گروهی دوری از مرتبهٔ n بوده و $k \mid n$ ، آنگاه G دقیقا" یک زیرگروه از مرتبهٔ k دارد.

۷ . فرض کنید p اول بوده و H زیرگروهی از $Z(p^\infty)$ باشد (تمرین ۱۰۰۱).

(آ) هر عنصر $Z(p^\infty)$ دارای مرتبهٔ متناهی p^n به‌ازای $n \geq 0$ ی می‌باشد.

(ب) هرگاه دست کم یک عنصر H دارای مرتبهٔ p^k بوده و H عنصری از مرتبهٔ بزرگتر از p^k نداشته باشد ، آنگاه H زیرگروه دوری تولید شده به وسیلهٔ $\overline{1/p^k}$ است ؛ درنتیجه ، $H \cong Z_{p^k}$.

(پ) هرگاه مرتبه‌های عناصر H کران بالایی نداشته باشند ، آنگاه $H = Z(p^\infty)$ [ر.ک. تمرین ۱۶۰۲] .

(ت) تنها زیرگروههای حقیقی $Z(p^\infty)$ گروههای دوری و متناهی $C_n = \langle \overline{1/p^n} \rangle$ $(n = 0,1,2,\ldots)$ می‌باشند ، به علاوه $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots$.

(ث) فرض کنید $x_1, x_2, \ldots$ عنصرهای یک گروه آبلی G باشند به‌طوری که $|x_1| = p, px_2 = x_1, px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$. زیرگروه تولید شده به وسیلهٔ $x_i (i \geq 1)$ با $Z(p^\infty)$ یکریخت است . [**راهنمایی** . تحقیق کنید که نگاشت القا شده

به وسیلهٔ $x_i \mapsto \overline{1/p_i}$ یکریختی تعریف شده‌ای است .]

۸ . هر گروه که تعدادی متناهی زیر گروه دارد باید متناهی باشد .

۹ . هرگاه G گروهی آبلی باشد ، آنگاه مجموعهٔ T مرکب از تمام عناصر G با مرتبهٔ متناهی زیرگروهی از G است . [با تمرین ۵ قیاس کنید .]

۱۰ . یک گروه نابدیهی دوری نامتناهی است اگر و فقط اگر با هر زیرگروه حقیقی خود یکریخت باشد .

۴ هم‌مجموعه‌ها و شمارش

در این بخش اولین قضیهٔ مهمی را به دست می‌آوریم که ساختار گروه متناهی G را با چند خاصیت نظریهٔ اعدادی $|G|$ پیوند می‌دهد . مطلب را با تعمیم مفهوم همنهشتی به پیمانهٔ m در گروه $\mathbf{Z}$ آغاز می‌کنیم . بنا بر تعریف ، $a \equiv b \pmod m$ اگر و فقط اگر $m \mid a - b$ ؛ یعنی ، اگر و فقط اگر $a - b$ عنصری از زیر گروه $\langle m \rangle = \{mk \mid k \in \mathbf{Z}\}$ باشد . به طور کلی (و با نماد ضربی) ، داریم

تعریف ۱۰۴ . فرض کنیم H زیرگروهی از گروه G بوده و $a, b \in G$. a همنهشت *راست* b به *پیمانهٔ* H است ، که با $a \equiv_r b \pmod H$ نموده می‌شود ، اگر $ab^{-1} \in H$. a همنهشت *چپ* b به *پیمانهٔ* H است ، که با $a \equiv_l b \pmod H$ نموده می‌شود ، اگر $a^{-1}b \in H$.

هرگاه G آبلی باشد ، آنگاه همنهشتی راست و چپ به پیمانهٔ H یکی‌اند (زیرا $ab^{-1} \in H \Leftrightarrow (ab^{-1})^{-1} \in H$ و $(ab^{-1})^{-1} = ba^{-1} = a^{-1}b$) . همچنین ، گروههای غیرآبلی G و زیرگروههای H وجود دارند به‌طوری‌که همنهشتی راست و چپ یکی‌اند (بخش ۵) ، ولی این در حالت کلی درست نیست .

قضیهٔ ۲۰۴ . *فرض کنیم H زیرگروهی از گروه G باشد .*

(یک) همنهشتی راست [چپ] به پیمانهٔ H یک رابطهٔ هم‌ارزی بر G است .

(دو) ردهٔ هم‌ارزی $a \in G$ تحت همنهشتی راست [چپ] به پیمانهٔ H مجموعهٔ $[aH = \{ah \mid h \in H\}]Ha = \{ha \mid h \in H\}$ است .

(سه) به‌ازای هر $a \in G$ ، $|Ha| = |H| = |aH|$.

مجموعهٔ Ha یک هم‌مجموعهٔ راست H در G ، و aH یک هم‌مجموعهٔ چپ H در

G نامیده می‌شود. در حالت کلی این طور نیست که هر هم‌مجموعهٔ راست هم‌مجموعهٔ چپ نیز باشد (تمرین ۲).

برهان ۲.۴. به‌جای $a \equiv b$ می‌نویسیم $a \equiv_H b \pmod H$ و قضیه را برای همنهشتی راست و هم‌مجموعه‌های راست ثابت می‌کنیم. استدلالهایی مشابه برای همنهشتی چپ اعمال می‌شود.

(یک) فرض کنیم $a,b,c \in G$. پس $a \equiv a$، زیرا $aa^{-1} = e \in H$؛ از اینرو، $\equiv$ منعکس است. $\equiv$ به وضوح متقارن است.

$$(a \equiv b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow b \equiv a).$$

بالاخره، $b \equiv c$ و $a \equiv b$ ایجاب می‌کنند که $ab^{-1} \in H$ و $bc^{-1} \in H$. لذا، $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$ و $a \equiv c$؛ از اینرو، $\equiv$ متعدی است. بنابراین، همنهشتی راست به پیمانهٔ H یک رابطهٔ هم‌ارزی است.

(دو) ردهٔ هم‌ارزی $a \in G$ تحت همنهشتی راست عبارت است از

$$\{x \in G \mid x \equiv a\} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h \in H\} = \{x \in G \mid x = ha; h \in H\} = \{ha \mid h \in H\} = Ha$$

(سه) به آسانی دیده می‌شود که نگاشت $Ha \to H$ داده شده با $ha \mapsto h$ یک بیژکسیون است.

نتیجهٔ ۲.۴. *فرض کنیم H زیرگروهی از گروه G باشد.*

(یک) G اجتماع هم‌مجموعه‌های راست [چپ] H در G است.

(دو) دو هم‌مجموعهٔ راست [چپ] H در G یا از هم جدایند یا مساوی.

(سه) به‌ازای هر $a,b \in G$، $Ha = Hb \Leftrightarrow ab^{-1} \in H$ و $aH = bH \Leftrightarrow a^{-1}b \in H$.

(چهار) هرگاه $\mathcal{R}$ مجموعهٔ هم‌مجموعه‌های راست متمایز H در G بوده و $\mathcal{L}$ مجموعهٔ هم‌مجموعه‌های چپ متمایز H در G باشد، آنگاه $|\mathcal{L}| = |\mathcal{R}|$.

برهان. قسمتهای (یک) تا (سه) نتایج فوری قضیه و احکام (۱۹) تا (۲۱) آشنایی، بخش ۴، اند. (چهار). نگاشت $\mathcal{L} \to \mathcal{R}$ داده شده با $Ha \mapsto a^{-1}H$ یک بیژکسیون است، زیرا

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H$$

نماد جمعی . هرگاه H زیرگروهی از یک گروه جمعی باشد، آنگاه همنهشتی راست به پیمانهٔ H به این صورت تعریف می‌شود: $a \equiv_r b \pmod{H} \Leftrightarrow a - b \in H$. ردهٔ همنهشتی $a \in G$ هم مجموعهٔ راست $H + a = \{h + a \mid h \in H\}$ است: مورد همنهشتی چپ و هم مجموعه‌های چپ به همین نحو می‌باشد.

تعریف ۴۰۴ . فرض کنیم H زیرگروهی از گروه G باشد. **اندیس H در G**، که با $[G : H]$ نموده می‌شود، عدد اصلی مجموعهٔ هم مجموعه‌های راست [چپ] متمایز از H در G است.

در پرتو نتیجهٔ ۳۰۴ (چهار)، $[G : H]$ به چپ و راستی هم مجموعه‌های به کار رفته در تعریف بستگی ندارد. توجه اصلی ما به حالتی است که $[G : H]$ متناهی است، که این حتی وقتی G و H گروههایی نامتناهی‌اند نیز رخ می‌دهد (مثلاً، طبق قضیهٔ ۸۰۶ (یک)، آشنایی، $[\mathbf{Z} : \langle m \rangle] = m$). توجه کنید هرگاه $H = \langle e \rangle$، آنگاه به‌ازای هر $a \in G$، $Ha = \{a\}$، و $[G : H] = |G|$.

یک **مجموعهٔ تام از نماینده‌های هم مجموعه‌های راست** یک زیر گروه H در گروه G مجموعه‌ای است مانند $\{a_i\}$ مرکب از دقیقاً یک عنصر از هر هم مجموعهٔ راست H در G. واضح است که مجموعهٔ $\{a_i\}$ دارای اصلیت $[G : H]$ است. توجه کنید که چنین مجموعه شامل دقیقاً یک عنصر از H است، زیرا $H = He$ خود یک هم مجموعهٔ راست است. احکام مشابهی در مورد هم مجموعه‌های چپ قابل بیانند.

قضیهٔ ۵۰۴ . *هرگاه K,H,G گروههایی با خاصیت $K < H < G$ باشند، آنگاه $[G : K] = [G : H][H : K]$. هرگاه دو تا از این اندیسها متناهی باشند، آنگاه سومی نیز چنین خواهد بود.*

برهان . بنابر نتیجهٔ ۳۰۴، $G = \bigcup_{i \in I} Ha_i$ با $a_i \in G$، $|I| = [G : H]$، و هم مجموعه‌های Ha_i دو به دو از هم جدایند (یعنی، $Ha_i = Ha_j \Leftrightarrow i = j$). به همین نحو، $H = \bigcup_{j \in J} Kb_j$ با $b_j \in H$، $|J| = [H : K]$، و هم مجموعه‌های Kb_j دو به دو از هم جدایند. بنابراین،

$G = \bigcup_{i\in I} Ha_i = \bigcup_{i\in I}(\bigcup_{j\in J} Kb_j)a_i = \bigcup_{(i,j)\in I\times J} Kb_ja_i$. کافی است نشان دهیم که هم‌مجموعه‌های Kb_ja_i دو بـه دو از هم جدایند. زیرا، دراین‌صورت، بنابر نتیجهٔ ۳.۴، باید داشته باشیم $[G:K] = |I\times J|$، که از آنجا

$$[G:K] = |I\times J| = |I||J| = [G:H][H:K].$$

هرگـاه $Kb_ja_i = Kb_ra_r$ آنـگاه $(k\in K).\ b_ja_i = kb_ra_r$. چـون $b_i,b_r,k\in H$، داریـم $Ha_i = Hb_ja_i = Hkb_ra_r = Ha_r$؛ ازاینرو، $i = r$ و $b_j = kb_r$. لذا، $Kb_j = Kkb_r = Kb_r$ و $j = r$. بنابراین، هم‌مجموعه‌های Kb_ja_i از هم‌جدایند. حکم دوم قضیه واضح است.

نتیجهٔ ۶.۴ (لاگرانژ[1]). *هرگاه H زیرگروهی از گروه G باشد، آنگاه* $|G| = [G:H]|H|$. *بخصوص، اگر G متناهی باشد، مرتبهٔ* $|a|$ *از* $a\in G$، $|G|$ *را عاد می‌کند.*

برهان. برای حکم اول، قضیه را به‌ازای $K = \langle e\rangle$ به کار برید. حکم دوم حالت خاصی از حکم اول است که در آن $H = \langle a\rangle$.

چند برهان در نظـریهٔ گروههای (متناهی) متکی به تکنیکهای مختلف "شمارش" می‌باشند، که اینک به معرفی برخی از آنهامی‌پردازیم. اگر G گروه و H,K زیرمجموعه‌هایی از G باشند، مجموعهٔ $\{ab \mid a\in H, b\in K\}$ را با HK نشان می‌دهیم؛ هم‌مجموعهٔ راست یا چپ یک زیرگروه حالت خاصی از آن است. اگر H,K زیرگروه باشند، HK ممکن است زیرگروه نباشد (تمرین ۷).

قضیهٔ ۷.۴. *فرض کنیم H و K زیرگروههایی متناهی از گروه G باشند. دراین‌صورت،* $|HK| = |H||K|/|H\cap K|$.

طرح برهان. $C = H\cap K$ زیرگروهی از K با اندیس $n = |K|/|H\cap K|$ بوده و K اجتماع از هم‌جدای هـم‌مجموعه‌های راسـت $Ck_1\cup Ck_2\cup\cdots\cup Ck_n$ به‌ازای $k_i\in K$، می‌باشد. چون $HC = H$، این ایجاب می‌کندکه HK اجتماع از هم‌جدای $Hk_1\cup Hk_2\cup\cdots\cup Hk_n$

---

1. *Lagrange*

باشد. بنابراین، $|HK| = |H| \cdot n = |H||K|/|H \cap K|$.

حکم ۸۰۴. *هرگاه H و K زیرگروههایی از گروه G باشند، آنگاه* $[H : H \cap K] \leq [G : K]$. *هرگاه* $[G : K]$ *متناهی باشد، آنگاه* $[H : H \cap K] = [G : K]$ *اگر و فقط اگر* $G = KH$.

طرح برهان. فرض کنیم A مجموعهٔ تمام هم‌مجموعه‌های راست $H \cap K$ در H و B مجموعهٔ تمام هم‌مجموعه‌های راست K در G باشد. نگاشت $\varphi : A \to B$ داده شده با $(H \cap K)h \mapsto Kh \quad (h \in H)$ تعریف شده است، زیرا $(H \cap K)h = (H \cap K)h'$ ایجاب می‌کند که $h'h^{-1} \in H \cap K \subset K$؛ و درنتیجه، $Kh' = Kh$. نشان دهید φ انژکتیو است. پس داریم، $[H : H \cap K] = |A| \leq |B| = [G : K]$ متناهی باشد، آنگاه نشان دهید که $[H : H \cap K] = [G : K]$ اگر و فقط اگر φ سورژکتیو باشد و φ سورژکتیو است اگر و فقط اگر $G = KH$. توجه کنید که به ازای $h \in H, k \in K$، $Kkh = Kh$، زیرا $(kh)h^{-1} = k \in K$.

حکم ۹۰۴. *فرض کنیم H و K زیرگروههایی از گروه G و با اندیس متناهی باشند. در این صورت،* $[G : H \cap K]$ *متناهی است و* $[G : H \cap K] \leq [G : H][G : K]$. *به علاوه،* $[G : H \cap K] = [G : H][G : K]$ *اگر و فقط اگر* $G = HK$.

برهان. تمرین؛ از قضیهٔ ۵۰۴ و حکم ۸۰۴ استفاده کنید.

تمرینات

۱. فرض کنید G یک گروه و $\{H_i \mid i \in I\}$ خانواده‌ای از زیرگروهها باشد. در این صورت به‌ازای هر $a \in G$، $(\bigcap_i H_i)a = \bigcap_i H_i a$.

۲. (آ) فرض کنید H زیرگروه دوری (از مرتبهٔ 2) از S_3 باشد که به وسیلهٔ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ تولید شده است. در این صورت، هیچ هم‌مجموعهٔ چپ H (جز خود H) هم‌مجموعهٔ راست نیست. عنصری مانند $a \in S_3$ وجود دارد به‌طوری که $aH \cap Ha = \{a\}$.

(ب) هرگاه K زیرگروه دوری (از مرتبهٔ 3) از S_3 باشد که به وسیلهٔ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

تولید شده باشد، آنگاه هر هم‌مجموعهٔ چپ K هم‌مجموعهٔ راست K نیز هست.

۳. شرایط زیر بر گروه متناهی G معادلند:
(یک) $|G|$ اول است؛
(دو) $G \neq \langle e \rangle$ و G زیرگروه حقیقی ندارد؛
(سه) به‌ازای عدد اولی مانند p، $G \cong Z_p$.

۴. (اویلر[1] ـ فرما[2]). فرض کنید a عددی صحیح و p عددی اول باشد به‌طوری که $p \nmid a$. در این صورت، $a^{p-1} \equiv 1 \pmod{p}$. [**راهنمایی.** $\bar{a} \in Z_p$ و گروه ضربی عناصر ناصفر Z_p را در نظر بگیرید؛ ر.ک. تمرین ۷.۱.] از آنجا نتیجه می‌شود که به‌ازای هر عدد صحیح مانند a، $a^p \equiv a \pmod{p}$.

۵. ثابت کنید فقط دو گروه متمایز از مرتبهٔ 4 (با تقریب یکریختی)، یعنی Z_4 و $Z_2 \oplus Z_2$، وجود دارند. [**راهنمایی.** طبق قضیهٔ لاگرانژ ۶.۴، یک گروه از مرتبهٔ 4 که دوری نباشد باید از همانی و سه عنصر از مرتبهٔ 2 تشکیل شده باشد.]

۶. فرض کنید H, K زیرگروههایی از گروه G باشند. در این‌صورت، HK زیرگروهی از G است اگر و فقط اگر $HK = KH$.

۷. فرض کنید G گروهی از مرتبهٔ $p^k m$ باشد، که در آن p اول بوده و $(p, m) = 1$. همچنین، H زیرگروهی از مرتبهٔ p^k و K زیرگروهی از مرتبهٔ p^d باشد، که $0 < d \leq k$، و $K \not\subset H$. نشان دهید که HK زیرگروهی از G نیست.

۸. هرگاه H و K زیرگروههایی از گروه G با اندیس متناهی باشند به‌طوری‌که $[G : H]$ و $[G : K]$ نسبت به هم اول باشند، آنگاه $G = HK$.

۹. هرگاه H، K، و N زیرگروههایی از گروه G باشند به‌طوری‌که $H < N$، آنگاه $HK \cap N = H(K \cap N)$.

۱۰. فرض کنید H, K, N زیرگروههایی از گروه G باشند به‌طوری‌که $H < K$، $H \cap N = K \cap N$، و $HN = KN$. نشان دهید که $H = K$.

۱۱. فرض کنید G گروهی از مرتبهٔ $2n$ باشد؛ در این‌صورت، G شامل عنصری از مرتبهٔ 2 است. اگر n فرد بوده و G آبلی باشد، فقط یک عنصر از مرتبهٔ 2 وجود دارد.

۱۲. هرگاه H و K زیرگروههایی از گروه G باشند، آنگاه $[H \vee K : H] \geq [K : H \cap K]$.

---

1. Euler 2. Fermat

۱۳ . اگر $p > q$ اعدادی اول باشند ، هرگروه از مرتبهٔ pq حداکثر یک زیرگروه از مرتبهٔ p دارد . [**راهنمایی** . فرض کنید H,K زیرگروههای متمایزی از مرتبهٔ p باشند . نشان دهید که $H \cap K = \langle e \rangle$ ؛ از تمرین ۱۲ استفاده کرده تناقض به دست آورید .]

۱۴ . فرض کنید G یک گروه و $a,b \in G$ چنان باشند که (یک) $|a| = 4 = |b|$ ؛ (دو) $a^2 = b^2$ ؛ (سه) $ba = a^3b = a^{-1}b$ ؛ (چهار) $a \neq b$ ؛ (پنج) $G = \langle a,b \rangle$. نشان دهید که $|G| = 8$ و $G \cong Q_8$. (ر.ک. تمرین ۳۰۲ ؛ توجه کنید که مولدهای A,B از Q_8 نیز در (یک) تا (چهار) صدق می‌کنند .)

۵ نرمالی ، گروههای خارج قسمتی ، و همریختیها

آن زیرگروههای N از گروه G را مطالعه می‌کنیم که همنهشتیهای چپ و راست به پیمانهٔ N یکی هستند . این نوع زیرگروهها نقش مهمی در تعیین ساختار یک گروه G و سرشت همریختیها با دامنهٔ G ایفا می‌کنند .

قضیهٔ ۱۰۵ . *هرگاه N زیرگروهی از گروه G باشد ، آنگاه شرایط زیر معادلند :*

(یک) همنهشتیهای چپ و راست به پیمانهٔ N یکی‌اند (یعنی ، یک رابطهٔ هم‌ارزی بر G تعریف می‌کنند) ؛

(دو) هر هم‌مجموعهٔ چپ N در G یک هم‌مجموعهٔ راست N در G است ؛

(سه) به‌ازای هر $a \in G$ ، $aN = Na$ ؛

(چهار) به‌ازای هر $a \in G$ ، $aNa^{-1} \subset N$ ، که در آن $aNa^{-1} = \{ana^{-1} \mid n \in N\}$ ؛

(پنج) به‌ازای هر $a \in G$ ، $aNa^{-1} = N$.

برهان (سه) $\Leftrightarrow$ (یک) . دو رابطهٔ هم‌ارزی R و S یکی‌اند اگر و فقط اگر ردهٔ هم‌ارزی هر عنصر تحت R مساوی ردهٔ هم‌ارزیش تحت S باشد . در این حالت رده‌های هم‌ارزی به ترتیب هم مجموعه‌های چپ و راست N اند .

(سه) $\Rightarrow$ (دو) . هرگاه به‌ازای $b \in G$ ای ، $aN = Nb$ ، آنگاه $a \in Nb \cap Na$ ، که ایجاب می‌کند $Nb = Na$ ، زیرا دو هم‌مجموعهٔ راست یا از هم جدایند یا مساوی.

(چهار) $\Rightarrow$ (سه) بدیهی است . (پنج) $\Rightarrow$ (چهار) . داریم $aNa^{-1} \subset N$. چون (چهار) به ازای $a^{-1} \in G$ نیز برقرار است ، $a^{-1}Na \subset N$. بنابراین ، به‌ازای هر $n \in N$ ،

$n = a(a^{-1}na)a^{-1} \in aNa^{-1}$ و $N \subset aNa^{-1}$. (دو) $\Rightarrow$ (پنج) فوراً حاصل می‌شود.

تعریف ۲۰۵. زیرگروه N از گروه G که در شرایط معادل قضیهٔ ۱۰۵ صدق کند در G **نرمال** (یا یک **زیرگروه نرمال** G) نامیده می‌شود؛ اگر N در G نرمال باشد، می‌نویسیم $N \lhd G$.

در پرتو قضیهٔ ۱۰۵، می‌توان زیرنویسهای "r" و "l" در همنهشتی به پیمانهٔ یک زیرگروه نرمال را حذف کرد.

چند مثال. هر زیرگروه یک گروه آبلی بداهتاً نرمال است. زیرگروه H تولید شده به وسیلهٔ $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ در S_3 نرمال است (تمرین ۲۰۴). به طورکلی، هر زیرگروه N با اندیس 2 در گروه G نرمال است (تمرین ۱). اشتراک هر خانواده از زیرگروههای نرمال یک زیرگروه نرمال است (تمرین ۲).

اگر G یک گروه و N و M زیرگروههای آن باشند به‌طوری‌که $N \lhd M$ و $M \lhd G$، نتیجه نمی‌شود که $N \lhd G$ (تمرین ۱۰). اما به‌آسانی دیده می‌شود که هرگاه N در G نرمال باشد، آنگاه N در هر زیرگروه G شامل N نیز نرمال است.

به یاد آورید که الحاق $H \vee K$ دو زیرگروه زیرگروه $\langle H \cup K \rangle$ تولید شده به وسیلهٔ H و K است.

قضیهٔ ۳۰۵. *فرض کنیم K و N زیرگروههایی از گروه G بوده و N در G نرمال باشد. در این صورت،*

(یک) $N \cap K$ یک زیرگروه نرمال K است؛

(دو) N زیرگروه نرمالی از $N \vee K$ است؛

(سه) $NK = N \vee K = KN$؛

(چهار) هرگاه K در G نرمال بوده و $N \cap K = \langle e \rangle$، آنگاه به‌ازای هر $k \in K$ و $n \in N$، $nk = kn$.

برهان (یک). هرگاه $n \in N \cap K$ و $a \in K$، آنگاه $ana^{-1} \in N$، زیرا $N \lhd G$ و $ana^{-1} \in K$،

زیرا $K < G$. لذا، $a(N \cap K)a^{-1} \subset N \cap K$ و $N \cap K \lhd K$. (دو) بدیهی است، زیرا $N < N \vee K$. (سه) واضح است که $NK \subset N \vee K$. عنصر x از $N \vee K$ حاصلضربی به شکل $n_1k_1n_2k_2\cdots n_rk_r$ است، که در آن $n_i \in N, k_i \in K$ (قضیهٔ ۸۰۲) . چون $N \lhd G$ ، $n_ik_j = k_jn_i'$ ، $n_i' \in N$ ؛ و درنتیجه، x را می‌توان به شکل $n(k_1\cdots k_r)$ ، $n \in N$ ، نوشت . لذا، $N \vee K \subset NK$. به همین نحو، $KN = N \vee K$. (چهار) فرض کنیم $k \in K$ و $n \in N$. پس $nkn^{-1} \in K$ ، زیرا $K \lhd G$ و $kn^{-1}k^{-1} \in N$ ، چون $N \lhd G$. از اینرو، $(nkn^{-1})k^{-1} = n(kn^{-1}k^{-1}) \in N \cap K = \langle e \rangle$ ، که $kn = nk$ را ایجاب می‌کند .

قضیهٔ ۴۰۵ . هرگاه N زیرگروه نرمالی از گروه G بوده و G/N مجموعهٔ تمام هم‌مجموعه‌های (چپ) N در G باشد، آنگاه G/N تحت عمل دوتایی داده شده با (aN)(bN) = abN گروهی از مرتبهٔ [G : N] است .

برهان . چون هم‌مجموعهٔ aN [یا bN, abN] چیزی جز ردهٔ هم‌ارزی $a \in G$ [یا $b \in G, ab \in G$] تحت رابطهٔ هم‌ارزی همنهشتی به پیمانهٔ N نیست، طبق قضیهٔ ۵۰۱ کافی است نشان دهیم که همنهشتی به پیمانهٔ N یک رابطهٔ هم‌ارزی است؛ یعنی، $a_1 \equiv a \pmod N$ و $b_1 \equiv b \pmod N$ ایجاب می‌کنند که $a_1b_1 \equiv ab \pmod N$. طبق فرض، $a_1a^{-1} = n_1 \in N$ و $b_1b^{-1} = n_2 \in N$. از اینرو،

$$(a_1b_1)(ab)^{-1} = a_1b_1b^{-1}a^{-1} = (a_1n_2)a^{-1}.$$

اما چون N نرمال است، داریم $a_1N = Na_1$ که ایجاب می‌کند که به‌ازای $n_3 \in N$ ای، $a_1n_2 = n_3a_1$. درنتیجه،

$$(a_1b_1)(ab)^{-1} = (a_1n_2)a^{-1} = n_3a_1a^{-1} = n_3n_1 \in N,$$

که از آنجا $a_1b_1 \equiv ab \pmod N$.

هرگاه N زیرگروه نرمالی از گروه G باشد، آنگاه گروه G/N ، همانند در قضیهٔ ۴۰۵ ، **گروه خارج‌قسمتی یا گروه عاملی** G بر N نامیده می‌شود . هرگاه G به‌طور جمعی نوشته شود، آنگاه‌عمل گروه در G/N با $(a + N) + (b + N) = (a + b) + N$ داده‌می‌شود .

تبصره . هرگاه $m > 1$ یک عدد صحیح (ثابت) بوده و $k \in \mathbf{Z}$ ، آنگاه نکات پیش‌از

تعریف ۱.۴ نشان می‌دهند که ردهٔ هم‌ارزی k تحت همنهشتی به پیمانهٔ m دقیقاً" هم‌مجموعهٔ $\langle m \rangle$ در $\mathbf{Z}$ است که شامل k می‌باشد؛ یعنی، به عنوان مجموعه، داریم $Z_m = \mathbf{Z}/\langle m \rangle$. قضایای ۵.۱ و ۴.۵ نشان می‌دهند که اعمال گروهی آنها یکی هستند، پس، به عنوان گروه، $Z_m = \mathbf{Z}/\langle m \rangle$.

حال به جستجوی روابط بین زیرگروههای نرمال، گروههای خارج قسمتی، و همریختیها می‌پردازیم.

قضیهٔ ۵.۵. *هرگاه $f: G \to H$ یک همریختی گروهها باشد، آنگاه هستهٔ f یک زیرگروه نرمال G است. به‌عکس، هرگاه N زیرگروه نرمالی از G باشد، آنگاه نگاشت $\pi : G \to G/N$ داده شده با $\pi(a) = aN$ یک بروریختی با هستهٔ N است.*

برهان. هرگاه $x \in \operatorname{Ker} f$ و $a \in G$، آنگاه

$$f(axa^{-1}) = f(a)\,f(x)\,f(a^{-1}) = f(a)ef(a)^{-1} = e$$

و $axa^{-1} \in \operatorname{Ker} f$. بنابراین، $a(\operatorname{Ker} f)a^{-1} \subset \operatorname{Ker} f$ و $\operatorname{Ker} f \lhd G$. نگاشت $\pi : G \to G/N$ به وضوح سورژکتیو است، و چون

$$\pi(ab) = abN = aNbN = \pi(a)\pi(b),$$

π یک بروریختی است.

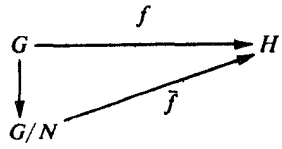
$$\operatorname{Ker} \pi = \{a \in G \mid \pi(a) = eN = N\} = \{a \in G \mid aN = N\} = \{a \in G \mid a \in N\} = N.$$

نگاشت $\pi : G \to G/N$ بروریختی **کانونی** یا **تصویر** نامیده می‌شود. از حالا به بعد، $G \to G/N$ $(N \lhd G)$ همواره بروریختی کانونی است مگر خلاف آن گفته شود.

قضیهٔ ۶.۵. *هرگاه $f: G \to H$ یک همریختی گروهها بوده و N زیرگروه نرمالی از G محتوا در هستهٔ f باشد، آنگاه همریختی منحصر به فردی مانند $\bar{f}: G/N \to H$ وجود دارد به‌طوری‌که به‌ازای هر $a \in G$، $\bar{f}(aN) = f(a)$، $Im\, f = Im\, \bar{f}$ و $Ker\, \bar{f} = (Ker\, f)/N$. $\bar{f}$ یکریختی است اگر و فقط اگر f یک بروریختی باشد و $N = Ker\, f$.*

قسمت اصلی نتیجه را می‌توان به صورتی دیگر گفت: همریختی منحصر به فردی

مانند $\bar{f}: G/N \to H$ وجود دارد به‌طوری‌که نمودار



تعویضپذیر است. نتیجهٔ ۸۰۵ در زیر را نیز می‌توان برحسب نمودارهای تعویضپذیر بیان کرد.

برهان ۶۰۵. هرگاه $b \in aN$، آنگاه $b = an$، $n \in N$، و $f(b) = f(an) = f(a)f(n) = f(a)e = f(a)$، زیرا $N < \operatorname{Ker} f$. بنابراین، f بر عناصر هم‌مجموعهٔ aN اثر یکسان داشته و نگاشت $\bar{f}: G/N \to H$ داده شده با $\bar{f}(aN) = f(a)$ تابع تعریف شده‌ای است. چون

$$\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN),$$

$\bar{f}$ یک همریختی است. واضح است که $\operatorname{Im} \bar{f} = \operatorname{Im} f$ و

$$aN \in \operatorname{Ker} \bar{f} \iff f(a) = e \iff a \in \operatorname{Ker} f,$$

که از آنجا $\operatorname{Ker} \bar{f} = \{aN \mid a \in \operatorname{Ker} f\} = (\operatorname{Ker} f)/N$. $\bar{f}$ منحصربه‌فرد است، زیرا کاملا" به وسیلهٔ f تعیین می‌شود. بالاخره، واضح است که $\bar{f}$ یک بروریختی است اگر و فقط اگر f چنین باشد. طبق قضیهٔ ۳۰۲، $\bar{f}$ تکریختی است اگر و فقط اگر $\operatorname{Ker} \bar{f} = (\operatorname{Ker} f)/N$ زیرگروه بدیهی G/N باشد، و این رخ می‌دهد اگر و فقط اگر $\operatorname{Ker} f = N$.

نتیجهٔ ۷۰۵ (قضیهٔ اول یکریختی). *هرگاه $f: G \to H$ یک همریختی از گروهها باشد، آنگاه f یکریختی $G/\operatorname{Ker} f \cong \operatorname{Im} f$ را القا می‌کند.*

برهان. $f: G \to \operatorname{Im} f$ یک بروریختی است. قضیهٔ ۶۰۵ را به‌ازای $N = \operatorname{Ker} f$ اعمال کنید.

نتیجهٔ ۸۰۵. *هرگاه $f: G \to H$ یک همریختی از گروهها باشد، $N \lhd G$، $M \lhd H$، و $f(N) < M$، آنگاه f یک همریختی مانند $\bar{f}: G/N \to H/M$ القا می‌کند که با*

$aN \mapsto f(a)M$ داده می‌شود . $\bar{f}$ یکریختی است اگر و فقط اگر $Im\, f \vee M = H$ و $f^{-1}(M) \subset N$. بخصوص، هرگاه f یک‌بروریختی باشد به‌طوری‌که $f(N) = M$ و $Ker\, f \subset N$ ، آنگاه $\bar{f}$ یکریختی است .

طرح برهان . ترکیب $G \xrightarrow{f} H \xrightarrow{\pi} H/M$ را در نظر گرفته و تحقیق کنید که $N \subset f^{-1}(M) = \text{Ker}\, \pi f$. طبق قضیهٔ ۶۰۵ (اعمال شده بر πf) ، نگاشت $G/N \to H/M$ داده شده با $aN \mapsto (\pi f)(a) = f(a)M$ یک همریختی است که یکریختی است اگر وفقط اگر πf بروریختی بوده و $N = \text{Ker}\, \pi f$. اما شرایط اخیر برقرار اند اگر وفقط اگر $\text{Im}\, f \vee M = H$ و $f^{-1}(M) \subset N$. هرگاه f یک بروریختی باشد ، آنگاه $H = \text{Im}\, f = \text{Im}\, f \vee M$. هرگاه $f(N) = M$ و $\text{Ker}\, f \subset N$ ، آنگاه $f^{-1}(M) \subset N$ ، که از آنجا $\bar{f}$ یک یکریختی می‌شود .

نتیجهٔ ۹۰۵ (قضیهٔ دوم یکریختی) . هرگاه K و N زیرگروههایی از گروه G بوده و N در G نرمال باشد ، آنگاه $K/(N \cap K) \cong NK/N$.

برهان . بنابر قضیهٔ ۳۰۵ ، $N \lhd NK = N \vee K$. ترکیب $K \hookrightarrow NK \xrightarrow{\pi} NK/N$ یک همریختی مانند f با هستهٔ $N \cap K$ است ، که از آنجا ، طبق نتیجهٔ ۷۰۵، $\bar{f}: K/K \cap N \cong \text{Im}\, f$ است . نرمالی N ایجاب می‌کند که $(n \in N, k \in K)\, nkN$ به شکل NK/N هر عنصر در $(n_1 \in N)\, nk = kn_1$ ، که از آنجا $nkN = kn_1N = kN = f(k)$. بنابراین ، f بروریختی است ؛ و در نتیجه ، $\text{Im}\, f = NK/N$.

نتیجهٔ ۱۰۰۵ (قضیهٔ سوم یکریختی) . هرگاه H و K زیرگروههای نرمال گروه G باشند به‌طوری‌که $K < H$ ، آنگاه H/K زیرگروه نرمالی از G/K بوده و $(G/K)/(H/K) \cong G/H$.

برهان . برای نگاشت همانی $1_G : G \to G$ داریم $1_G(K) < H$ ؛ ولذا ، یک بروریختی مانند $I : G/K \to G/H$ با ضابطهٔ $I(aK) = aH$ القا می‌کند . چون $H = I(aK)$ اگر و فقط اگر $a \in H$ ، $H/K \lhd G/K$ و ، درنتیجه ، طبق قضیهٔ ۵۰۵ ، $\text{Ker}\, I = \{aK \mid a \in H\} = H/K$. بنابر نتیجهٔ ۷۰۵ ، $G/H = \text{Im}\, I \cong (G/K)/\text{Ker}\, I = (G/K)/(H/K)$.

قضیهٔ ۱۱۰۵ . هرگاه $f : G \to H$ یک‌بروریختی گروهها باشد ، آنگاه ارتباط $K \mapsto f(K)$

تناظر یک بـه یکی بین مجموعهٔ $S_f(G)$ تمام زیرگروههای K از G که شامل $Ker\ f$ اند و مجموعهٔ $S(H)$ تمام‌زیرگروههای H تعریف‌می‌کند. تحت‌این‌تناظر یک‌به‌یک، زیرگروههای نرمال متناظر زیرگروههای نرمال می‌باشند.

طرح برهان. بنابرتمرین ۹۰۲، ارتباط $K \mapsto f(K)$ تابعی مانند $\varphi : S_f(G) \to S(H)$ تعریف می‌کندو $f^{-1}(J)$، به‌ازای هرزیرگروه J از H، زیرگروهی از G است. چون $J < H$ ایجاب می‌کند که $\operatorname{Ker} f < f^{-1}(J)$ و $f(f^{-1}(J)) = J$، φ سورژکتیو است. تمرین ۱۸ نشان می‌دهد که $f^{-1}(f(K)) = K$ اگر و فقط اگر $\operatorname{Ker} f < K$. پس نتیجه می‌شود که φ انژکتیو است. برای اثبات حکم دوم تحقیق می‌کنید که $K \lhd G$ ایجاب می‌کند $f(K) \lhd H$ را و $J \lhd H$ ایجاب می‌کند $f^{-1}(J) \lhd G$ را.

نتیجهٔ ۱۲۰۵. *هرگاه N زیرگروه نرمالی از گروه G باشد، آنگاه هر زیرگروه G/N به شکل K/N است، که درآن K زیرگروهی از G شامل N است. به‌علاوه، K/N در G/N نرمال است اگر و فقط اگر K در G نرمال باشد.*

برهان. قضیهٔ ۱۱۰۵ را بـر بـروریختی کانونی $\pi : G \to G/N$ اعمال می‌کنیم. هرگاه $N < K < G$، آنگاه $\pi(K) = K/N$.

تمرینات

۱. هرگاه N زیرگروهی با اندیس 2 در گروه G باشد، آنگاه N در G نرمال است.

۲. هرگاه $\{N_i \mid i \in I\}$ خانـواده‌ای از زیـرگروههای نـرمال گروه G باشد، آنگاه $\bigcap_{i \in I} N_i$ زیرگروه نرمالی از G است.

۳. فرض‌کنید N زیرگروهی‌ازگروه G باشد. N در G نرمال‌است‌اگرو فقط‌اگر همنهشتی (راست) به پیمانهٔ N یک رابطهٔ همنهشتی بر G باشد.

۴. فرض‌کنید $\sim$ رابطه‌ای هـم‌ارزی بر گروه G بوده و $N = \{a \in G \mid a \sim e\}$. $\sim$ یک رابطهٔ همنهشتـی بـر G است اگـر و فقط‌اگر N یک زیرگروه نرمال G بوده و $\sim$ همنهشتی به پیمانهٔ N باشد.

۵. فرض‌کنید $N < S_4$ مرکب از تمام‌جایگشتهای σ باشد کـه $\sigma(4) = 4$. آیـا N در S_4

نرمال است؟

۶ . فرض کنید $H < G$ ؛ پس مجموعهٔ aHa^{-1}، به‌ازای هر $a \in G$ یک زیر گروه است ، و $H \cong aHa^{-1}$.

۷ . فرض کنید G گروهی متناهی بوده و H یک زیرگروه G از مرتبهٔ n باشد . هرگاه H تنها زیرگروه G از مرتبهٔ n باشد ، آنگاه H در G نرمال است .

۸ . تمام زیرگروههای گروه چهارتایی نرمالند (ر.ک. تمرینهای ۳۰۲ و ۱۴۰۴) .

۹ . (آ) هرگاه G یک گروه باشد ، آنگاه مرکز G یک زیر گروه نرمال G است (ر.ک. تمرین ۱۱۰۲) ؛

(ب) به‌ازای هر $n > 2$ ، مرکز S_n زیرگروه همانی است .

۱۰ . زیرگروههای H و K از D_4^* را چنان بیابید که $H \lhd K$ و $K \lhd D_4^*$ ، ولی H در D_4^* نرمال نباشد .

۱۱ . هرگاه H یک‌زیرگروه‌دوری‌ازگروه G بوده و H در G نرمال باشد ، آنگاه هر زیرگروه H در G نرمال است . [قس. تمرین ۱۰۱۰]

۱۲ . هرگاه H یک زیرگروه نرمال‌گروه G باشد به‌طوری‌که H و G/H با تولید متناهی باشند ، آنگاه G نیز چنین است .

۱۳ . (آ) فرض کنید $H \lhd G, K \lhd G$. نشان دهید که $H \vee K$ در G نرمال است .

(ب) ثابت کنید مجموعهٔ تمام زیرگروههای نرمال G تحت شمول یک شبکهٔ تام تشکیل می‌دهد (تمرین ۲۰۷، آشنایی) .

۱۴ . هرگاه $N_1 \lhd G_1, N_2 \lhd G_2$ ، آنگاه $(N_1 \times N_2) \lhd (G_1 \times G_2)$ و $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$

۱۵ . فرض کنید $N \lhd G$ و $K \lhd G$. هرگاه $N \cap K = \langle e \rangle$ و $N \vee K = G$ ، آنگاه $G/N \cong K$.

۱۶ . هرگاه $f: G \to H$ یک‌همریختی ، H آبلی ، و N زیرگروهی‌از G شامل $\operatorname{Ker} f$ باشد ، آنگاه N در G نرمال است .

۱۷ . (آ) زیرگروههای $\langle 6 \rangle$ و $\langle 30 \rangle$ از $\mathbf{Z}$ را درنظرگرفته‌ونشان دهید که $\langle 6 \rangle / \langle 30 \rangle \cong Z_5$.

(ب) به‌ازای هر $k, m > 0$ ، $\langle k \rangle / \langle km \rangle \cong Z_m$ ؛ بخصوص، $\mathbf{Z}/\langle m \rangle = \langle 1 \rangle / \langle m \rangle \cong Z_m$.

۱۸ . هرگاه $f: G \to H$ یک همریختی با هستهٔ N بوده و $K < G$ ، آنگاه ثابت کنید که $f^{-1}(f(K)) = KN$. از اینرو ، $f^{-1}(f(K)) = K$ اگر و فقط‌اگر $N < K$.

۱۹ . هرگاه $N \lhd G$ ، $[G:N]$ متناهی باشد ، $H < G$ ، $|H|$ متناهی باشد ، و $[G:N]$ و $|H|$ نسبت به هم اول باشند ، آنگاه $H < N$.

۲۰ . هرگاه $N \lhd G$ ، $|N|$ متناهی باشد ، $H < G$ ، $[G:H]$ متناهی باشد ، و $[G:H]$ و $|N|$ نسبت به هم اول باشند ، آنگاه $N < H$.

۲۱ . هرگاه H زیرگروهی از $Z(p^\infty)$ بوده و $H \neq Z(p^\infty)$ ، آنگاه $Z(p^\infty)/H \cong Z(p^\infty)$.
[**راهنمایی** . اگر $H = \langle \overline{1/p^n} \rangle$ ، قرار دهید $x_i = \overline{1/p^{n+i}} + H$ و تمرین ۷۰۳ (ث) را به کار گیرید .]

۶ گروههای متقارن ، متناوب ، و دو وجهی

در این بخش به بررسی مشروح گروه متقارن S_n و بعضی از زیرگروههای آن می‌پردازیم . بنابر تعریف ، S_n گروه تمام بیژکسیونهای $I_n \to I_n$ است ، که در آن $I_n = \{1,2,\ldots,n\}$. عناصر S_n **جایگشت** نامیده می‌شوند . علاوه بر نماد صفحهٔ ۳۹ برای جایگشتها در S_n ، نماد متعارف دیگری‌نیز وجود دارد :

تعریف ۱۰۶ . فرض کنیم $(r \leq n) i_1, i_2, \ldots, i_r$ عنصرهای متمایزی از $I_n = \{1,2,\ldots n\}$ باشند . $(i_1 i_2 i_3 \cdots i_r)$ جایگشتی است که $i_1 \mapsto i_2$ ، $i_2 \mapsto i_3$ ، $i_3 \mapsto i_4$ ، . . . ، $i_{r-1} \mapsto i_r$ ، و $i_r \mapsto i_1$ ، و هر عنصر دیگری از I_n را به روی خودش می‌نگارد . $(i_1 i_2 \cdots i_r)$ یک **دور** به طول r یا یک rـ**دور** نامیده می‌شود ؛ هر 2ـ دور یک **ترانهش** نام دارد .

نماد دور منحصر به فرد نیست (ر . ک . زیر) ؛ درواقع ، به بیان دقیق ، نماد دور مبهم است ، زیرا $(i_1 \cdots i_r)$ ممکن است عنصری از S_n ، $n \geq r$ ، باشد . اما این مشکلی ایجاد نمی‌کند . هر 1ـ دور (k) جایگشت همانی است . واضح است که هر rـ دور عنصری از مرتبهٔ r در S_n است . همچنین ، می‌بینیم که اگر τ یک دور بوده و به ازای $x \in I_n$ ی ، $\tau(x) \neq x$ ، به‌ازای $d \geq 1$ ای داریم $\tau = (x\tau(x)\tau^2(x)\cdots\tau^d(x))$. معکوس دور $(i_1 i_2 \cdots i_r)$ دور $(i_r i_{r-1} i_{r-2} \cdots i_2 i_1) = (i_1 i_r i_{r-1} i_{r-2} \cdots i_2)$ است (تحقیق کنید !) .

چند مثال . جایگشت $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ یک 4ـ دور است :

$(2143) = (3214) = (4321) = (1432) = \tau$. هرگاه σ ، 3ـ دور (125) باشد ، آنگاه $\sigma\tau = (125)(1432) = (1435)$ (به یاد آورید که جایگشتها تابعند و $\sigma\tau$ یعنی τ و بعد از آن σ) ؛ به همین نحو ، $\tau\sigma = (1432)(125) = (2543)$ ؛ درنتیجه ، $\sigma\tau \neq \tau\sigma$. اما حالتی وجود دارد که در آن دو جایگشت با هم تعویض می‌شوند .

تعریف ۳۰۶ . جایگشتهای $\sigma_1,\sigma_2,\ldots,\sigma_r$ از S_n را *از هم جدا* گویند اگر به‌ازای هر $1 \leq i \leq r$ و هر $k \in I_n$ ، $\sigma_i(k) \neq k$ ایجاب کند که به ازای هر $j \neq i$ ، $\sigma_j(k) = k$.

به عبارت دیگر ، $\sigma_1,\sigma_2,\ldots,\sigma_r$ از هم جدایند اگر و فقط اگر هیچ عنصری از I_n به وسیلهٔ بیش از یکی از $\sigma_1,\ldots,\sigma_r$ حرکت نکند . به‌آسانی می‌بینیم که هر وقت σ و τ از هم جدا باشند ، $\tau\sigma = \sigma\tau$.

قضیهٔ ۳۰۶ . *هر جایگشت غیرهمانی در S_n را (صرف‌نظر از ترتیب عاملها) می‌توان به صورت حاصل ضربی منحصر به فرد از دورهای از هم جدا ، هر یک دست کم به طول 2 ، بیان کرد .*

طرح برهان . فرض کنیم $\sigma \in S_n$, $\sigma \neq (1)$. تحقیق کنید که رابطهٔ زیر یک رابطهٔ هم‌ارزی بر I_n است : به‌ازای $x,y \in I_n$ ، $x \sim y$ اگر و فقط اگر به‌ازای $m \in \mathbf{Z}$ ی ، $y = \sigma^m(x)$. رده‌های هم‌ارزی $\{B_i \mid 1 \leq i \leq s\}$ این رابطهٔ هم‌ارزی *مدارهای* σ نام دارند و افرازی از I_n را تشکیل می‌دهند (آشنایی ، قضیهٔ ۱۰۴) . توجه کنید که هرگاه $x \in B_i$ ، $B_i = \{u \mid x \sim u\} = \{\sigma^m(x) \mid m \in \mathbf{Z}\}$. فرض کنیم $(1 \leq r \leq s)$ $B_1,B_2,\ldots,B_r$ آن مدارهایی باشند که بیش از یک عنصر دارند ($r \geq 1$ ، زیرا $\sigma \neq (1)$) . به‌ازای هر $i \leq r$ $\sigma_i \in S_n$ را به صورت زیر تعریف می‌کنیم :

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{اگر } x \in B_i \\ x & \text{اگر } x \notin B_i \end{cases}$$

هر σ_i یک جایگشت غیرهمانی تعریف شده از I_n است ، زیرا $\sigma \mid B_i$ یک بیژکسیون $B_i \to B_i$ است . $\sigma_1,\sigma_2,\ldots,\sigma_r$ جایگشتهای از هم جدایی هستند ، زیرا مجموعه‌های $B_1,\ldots,B_r$ دو به دو از هم جدایند . بالاخره ، تحقیق کنید که $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ (توجه کنید که $x \in B_i$

ایجاب می‌کند که $\sigma(x) = \sigma_i(x)$ اگر $i \leq r$ و $\sigma(x) = x$ اگر $i > r$: خاصیت از هم جدایی را مورد استفاده قرار دهید) . باید نشان دهیم که هر σ_i یک دور است . هرگاه $x \in B_i$ $(i \leq r)$ ، آنگاه چون B_i متناهی است ، کوچکترین عدد صحیح مثبتی مانند d هست به‌طوری‌که‌به‌ازای j ای $(0 \leq j < d)$ ، $\sigma^d(x) = \sigma^j(x)$. چون $\sigma^{d-j}(x) = x$ و $0 < d - j \leq d$ باید داشته باشیم $\sigma^d(x) = x$ و $j = 0$. ازاینرو ، $(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x))$ یک دور تعریف شده باطول دست‌کم 2 است . هرگاه $\sigma^m(x) \in B_i$ ، آنگاه‌به‌ازای $a,b \in \mathbf{Z}$ ای ، $m = ad + b$ به‌طوری‌که $0 \leq b < d$. از اینرو ،

$$\sigma^m(x) = \sigma^{b+ad}(x) = \sigma^b\sigma^{ad}(x) = \sigma^b(x) \in \{x,\sigma(x),\sigma^2(x),\ldots,\sigma^{d-1}(x)\}.$$

بنابراین ، $B_i = \{x,\sigma(x),\sigma^2(x),\ldots,\sigma^{d-1}(x)\}$ و نتیجه می‌شود که σ_i دور

$$(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x))$$

می‌باشد .

فرض کنیم $\tau_1,\ldots,\tau_t$ دورهای از هم جدایی باشند به‌طوری که $\sigma = \tau_1\tau_2\cdots\tau_t$. همچنین ، $x \in I_n$ به‌طوری‌که $\sigma(x) \neq x$. طبق از هم جدایی ، j ی منحصر به فردی $(1 \leq j \leq t)$ باخاصیت $\sigma(x) = \tau_j(x)$ وجود دارد . چون $\sigma\tau_j = \tau_j\sigma$ ، به‌ازای هر $k \in \mathbf{Z}$ داریم $\sigma^k(x) = \tau_j^k(x)$. بنابراین ، مدار x تحت τ_j درست مدار x تحت σ ، مثلا" B_i ، است . در نتیجه ، به‌ازای هر $y \in B_i$ ، $\tau_j(y) = \sigma(y)$ (زیرا به‌ازای $n \in \mathbf{Z}$ ی ، $(y = \sigma^n(x) = \tau_j^n(x)$) . چون τ_j یک‌دوراست ، فقط یک‌مدارنابدیهی‌دارد (تحقیق کنید!) ، که باید B_i باشد ، زیرا $x \neq \sigma(x) = \tau_j(x)$. بنابراین ، به‌ازای هر $y \notin B_i$ ، $\tau_j(y) = y$ ، که از آنجا $\tau_j = \sigma_i$. استدلال استقرایی مناسبی نشان می‌دهد که $r = t$ و (پس‌از اندیسگذاری مجدد) ، به‌ازای هر $i = 1,2,\ldots,r$ ، $\sigma_i = \tau_i$.

نتیجهٔ ۴۰۶ . مرتبهٔ جایگشت $\sigma \in S_n$ کوچکترین مضرب مشترک مرتبه‌های دورهای از هم‌جدای آن است .

برهان . فرض کنیم $\sigma = \sigma_1\cdots\sigma_r$ ، که‌درآن $\{\sigma_i\}$ دورهای از هم جدایی می‌باشند . چون دورهای از هم جدا تعویض می‌شوند ، به‌ازای هر $m \in \mathbf{Z}$ ، $\sigma^m = \sigma_1^m\cdots\sigma_r^m$ و $\sigma^m = (1)$ اگر و فقط اگر به‌ازای هر i ، $\sigma_i^m = (1)$. بنابراین ، $\sigma^m = (1)$ اگر و فقط‌اگر $\{\sigma_i\}$ ، به ازای هر i ، m را عاد کند (قضیهٔ ۴۰۳) . چون $|\sigma|$ مینیمم این m هاست ، نتیجه

به دست خواهد آمد.

نتیجهٔ ۵.۶. *هر جایگشت در S_n را می‌توان به صورت حاصلضربی (نه لزوماً "از هم جدا") از ترانهشها نوشت.*

برهان. بنابر قضیهٔ ۳.۶، کافی است نشان دهیم که هر دور حاصلضربی از ترانهشهاست. این کار آسان است: $(x_1) = (x_1x_2)(x_1x_2)$ و، به‌ازای $r > 1$،

$$(x_1x_2x_3\cdots x_r) = (x_1x_r)(x_1x_{r-1})\cdots(x_1x_3)(x_1x_2).$$

تعریف ۶.۶. گوییم جایگشت $\tau \in S_n$ زوج [فرد] است اگر τ را بتوان به‌صورت حاصلضرب تعدادی زوج [فرد] از ترانهش نوشت.

علامت ترانهش τ، که با $\operatorname{sgn}\tau$ نموده می‌شود، بسته به زوج یا فرد بودن τ 1 یا 1− است. اینکه $\operatorname{sgn}\tau$ تعریف شده است نتیجهٔ فوری قضیهٔ زیر است.

قضیهٔ ۷.۶. *یک جایگشت در S_n $(n \geq 2)$ نمی‌تواند هم‌زوج و هم فرد باشد.*

برهان. فرض کنیم $i_1, i_2, \ldots, i_n$ اعداد صحیح $1,2,\ldots,n$ با ترتیبی خاص بوده و $\Delta(i_1,\ldots,i_n)$ را عدد صحیح $\prod (i_j - i_k)$ تعریف می‌کنیم، که در آن حاصلضرب روی تمام جفتهای (j,k) گرفته می‌شود که $1 \leq j < k \leq n$. توجه کنید که $\Delta(i_1,\ldots,i_n) \neq 0$. ابتدا $\Delta(\sigma(i_1),\ldots,\sigma(i_n))$ را وقتی $\sigma \in S_n$ یک ترانهش است، مثلاً "$\sigma = (i_ci_d)$ با $c < d$"، حساب می‌کنیم. داریم $\Delta(i_1,\ldots,i_n) = (i_c - i_d)ABCDEFG$، که در آن

$$A = \prod_{\substack{j<k \\ j,k\neq c,d}} (i_j - i_k); \quad B = \prod_{j<c} (i_j - i_c); \quad C = \prod_{j<c} (i_j - i_d);$$

$$D = \prod_{c<j<d} (i_j - i_d); \quad E = \prod_{c<k<d} (i_c - i_k); \quad F = \prod_{d<k} (i_c - i_k);$$

$$G = \prod_{d<k} (i_d - i_k).$$

به جای $\prod_{\substack{j<k \\ j,k\neq c,d}} (\sigma(i_j) - \sigma(i_k))$ می‌نویسیم $\sigma(A)$ و به‌همین‌ترتیب درمورد $\sigma(B)$، $\sigma(C)$،

و غیره. تحقیق کنید که $\sigma(A) = A$ ؛ $\sigma(B) = C$ و $\sigma(C) = B$ و $\sigma(D) = (-1)^{d-c-1}E$ ؛ $\sigma(E) = (-1)^{d-c-1}D$ ؛ $\sigma(F) = G$ و $\sigma(G) = F$. بالاخره ، $\sigma(i_c - i_d) = \sigma(i_c) - \sigma(i_d) =$ $i_d - i_c = -(i_c - i_d)$. درنتیجه ،

$$\Delta(\sigma(i_1), \ldots, \sigma(i_n)) = \sigma(i_c - i_d)\sigma(A)\sigma(B)\cdots\sigma(G) = (-1)^{1+2(d-c-1)}(i_c - i_d)ABCDEFG$$
$$= -\Delta(i_1, \ldots, i_n).$$

فرض کنیم بـه ازای $\tau \in S_n$ ای ، $\tau = \tau_1 \cdots \tau_r$ و $\tau = \sigma_1 \cdots \sigma_s$ کـه در آنها τ_i, σ_j ترانهش‌اند و r زوج و s فرد است . دراین‌صورت ، به‌ازای $(i_1, \ldots, i_n) = (1,2, \ldots, n)$ ، از بند قبل نتیجه می‌شود که

$$\Delta(\tau(1), \ldots, \tau(n)) = \Delta(\tau_1 \cdots \tau_r(1), \ldots, \tau_1 \cdots \tau_r(n)) = -\Delta(\tau_2 \cdots \tau_r(1), \ldots,$$
$$\tau_2 \cdots \tau_r(n)) = \cdots = (-1)^r\Delta(1,2, \ldots, n) = \Delta(1,2, \ldots, n).$$

به همین نحو ، $\Delta(\tau(1), \ldots, \tau(n)) = (-1)^s\Delta(1,2, \ldots, n) = -\Delta(1,2, \ldots, n)$ ، کـه از آنجا $\Delta(1,2, \ldots, n) = -\Delta(1,2, \ldots, n)$. این یک تناقض است ، زیرا $\Delta(1,2, \ldots, n) \neq 0$.

قضیهٔ ۸۰۶ . *به‌ازای هـر $n \geq 2$ ، فرض کنیم A_n مجموعهٔ تمام جایگشتهای زوج S_n باشد . A_n یک زیرگروه نرمال S_n با اندیس 2 و مرتبهٔ $|S_n|/2 = n!/2$ است . به علاوه ، A_n تنها زیرگروه S_n با اندیس 2 است .*

گروه A_n *گروه متناوب بر* **n** *حرف یا گروه متناوب از درجهٔ* **n** نامیده می‌شود .

طرح برهان **۸۰۶** . فرض کنیم C زیرگروه ضربی $\{1,-1\}$ از اعداد صحیح باشد . نگاشت $f: S_n \to C$ را بـا $\sigma \mapsto \operatorname{sgn}\sigma$ تعریف کـرده و تحقیق کنید f یک برووریختی گروههاست . چون هستهٔ f به وضوح A_n است ، A_n در S_n نرمال است . بنابر قضیهٔ اول یکریختی ، $S_n/A_n \cong C$ ، که ایجاب می‌کند $[S_n : A_n] = 2$ و $|A_n| = |S_n|/2$. بنـابر تمرین ۶ ، A_n زیرگروه منحصر به فرد S_n از مرتبهٔ 2 است .

تعریف ۹۰۶ . گروه G را *ساده* گویند اگر G زیرگروه نرمال حقیقی نداشته باشد .

تنها گروههای آبلی ساده عبارتند از Z_p با p اول (تمرین ۳۰۴) . گروههای سادهٔ

غیرآبلی وجود دارند ؛ بخصوص، داریم

قضیهٔ ۱۰.۶ . گروه متناوب A_n ساده است اگر و فقط اگر $n \neq 4$.

برهانی که خواهیم آورد نسبتا " مقدماتی است . قبلا " دولم می‌آوریم . به یاد آورید که اگر τ یک 2- دور باشد ، $\tau^2 = (1)$ ؛ و درنتیجه ، $\tau = \tau^{-1}$.

لم ۱۱.۶ . فرض کنیم r,s عناصر متمایزی از $\{1,2,\ldots,n\}$ باشند . در این صورت ، A_n $(n \geq 3)$ به وسیلهٔ 3- دورهای $\{(rsk) \mid 1 \leq k \leq n, k \neq r,s\}$ تولید می‌شود .

برهان . فرض کنیم $n > 3$ (حالت $n = 3$ بدیهی است) . هر عنصر A_n حاصلضرب جملاتی به شکل $(ab)(cd)$ یا $(ab)(ac)$ است ، که در آن a,b,c,d عنصرهای متمایزی‌از $\{1,2,\ldots,n\}$ می‌باشند . چون $(ab)(cd) = (acb)(acd)$ و $(ab)(ac) = (acb)$ ، A_n به وسیلهٔ مجموعهٔ تمام 3- دورها تولید می‌شود . هر 3- دور به شکل (rsa) ، (ras) ، (rab) ، (sab) ، یا (abc) است ، که در آنها a,b,c متمایز بوده و $a,b,c \neq r,s$. چون $(ras) = (rsa)^2$ ، $(rab) = (rsb)(rsa)^2$ ، $(sab) = (rsb)^2(rsa)$ ، و $(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$ ، A_n به وسیلهٔ

$$\{(rsk) \mid 1 \leq k \leq n, k \neq r,s\}$$

تولید می‌شود .

لم ۱۲.۶ . هرگاه N زیرگروه نرمالی‌از A_n $(n \geq 3)$ بوده‌و N شامل‌یک 3- دورباشد ، آنگاه $N = A_n$.

برهان . هرگاه $(rsc) \in N$ ، آنگاه به‌ازای هر $k \neq r,s,c$ ،

$$(rsk) = (rs)(ck)(rsc)^2(ck)(rs) = [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N .$$

از اینرو ، بنابر لم ۱۱.۶ ، $N = A_n$.

برهان قضیهٔ ۱۰.۶ . $A_2 = (1)$ و A_3 گروه دوری ساده‌ای از مرتبهٔ 3 است . به آسانی

تحقیق می‌شود که $\{(1),(12)(34),(13)(24),(14)(23)\}$ زیرگروه نرمال A_4 است (تمرین ۷) . اگر $n \geq 5$ و N یک زیرگروه نرمال نابدیهی از A_n باشد، با توجه به حالات ممکن نشان خواهیم داد که $N = A_n$.

حالت ۱. N شامل یک 3- دور است؛ از اینرو، طبق لم ۱۲.۶ ، $N = A_n$.

حالت ۲. N شامل عنصری مانند σ است، به صورت حاصلضرب دورهای از هم جدا، که دست کم یکی از آنها به طول $r \geq 4$ است. لذا، $\sigma = (a_1a_2\cdots a_r)\tau$ (از هم جدا) . فرض کنیم $\delta = (a_1a_2a_3) \in A_n$. دراین‌صورت، بنابر نرمالی، $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$. اما

$$\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_1a_ra_{r-1}\cdots a_2)(a_1a_2a_3)(a_1a_2\cdots a_r)\tau(a_1a_3a_2) = (a_1a_3a_r) \in N.$$

لذا، طبق لم ۱۲.۶ ، $N = A_n$.

حالت ۳. N شامل عنصری‌است مانند σ ، به‌صورت حاصل ضربی از دورهای از هم جدا، که دست‌کم دوتای آنها طول 3 دارند؛ درنتیجه، (از هم جدا) $\sigma = (a_1a_2a_3)(a_4a_5a_6)\tau$. فرض کنیم $\delta = (a_1a_2a_4) \in A_n$. دراین‌صورت، مثل بالا، N شامل

$$\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)\tau\ (a_1a_4a_2) = (a_1a_4a_2a_6a_3)$$

است. از اینرو، طبق حالت ۲ ، $N = A_n$.

حالت ۴. N شامل عنصری مانند σ است، به صورت حاصل‌ضربی از یک 3- دور و چند 2- دور، مثلاً " (از هم جدا) $\sigma = (a_1a_2a_3)\tau$ ، که در آن τ حاصل‌ضربی از 2- دورهای از هم جداست. در این صورت، $\sigma^2 \in N$ و

$$\sigma^2 = (a_1a_2a_3)\tau(a_1a_2a_3)\tau = (a_1a_2a_3)^2\tau^2 = (a_1a_2a_3)^2 = (a_1a_3a_2)$$ ،

که از آنجا، بنابر لم ۱۲.۶ ، $N = A_n$.

حالت ۵. هر عنصر N حاصلضرب تعدادی (زوج) از 2- دورهای از هم جداست. فرض کنیم $\sigma \in N$ به‌صورت (از هم جدا) $\sigma = (a_1a_2)(a_3a_4)\tau$ باشد. همچنین، $\delta = (a_1a_2a_3) \in A_n$ ؛ دراین‌صورت، مثل بالا، $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ ، اما $\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_3a_4)(a_1a_2)(a_1a_2a_3)(a_1a_2)$ $= (a_3a_4)\tau(a_1a_3a_2) = (a_1a_3)(a_2a_4)$ ، چون $n \geq 5$ ، عنصری مانند $b \in \{1,2,\ldots,n\}$ متمایز از a_1,a_2,a_3,a_4 وجود دارد. چون $\xi = (a_1a_3b) \in A_n$ و $\zeta = (a_1a_3)(a_2a_4) \in N$ ، داریم $\zeta(\xi\zeta\xi^{-1}) \in N$. اما داریم $\zeta(\xi\zeta\xi^{-1}) = (a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)$ $= (a_2a_4)(a_1ba_3) = (a_1a_3b) \in N$. از اینرو، بنابر لم ۱۲.۶ ، $N = A_n$.

چون حالات فوق جمیع حالات ممکنه است، A_n زیرگروه نرمال حقیقی ندارد؛ و

درنتیجه، ساده است.

زیرگروه مهم دیگر S_n $(n \geq 3)$ زیرگروه D_n تولید شده به وسیلهٔ $a = (123\cdots n)$ و

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}$$
$$= \prod_{2 \leq i < n+2-i} (i \; n+2-i)$$

است. D_n **گروه دو وجهی از درجهٔ n** نامیده می‌شود. گروه D_n با گروه تمام تقارنهای یک n ضلعی منتظم یکریخت است و معمولاً با آن یکی گرفته می‌شود (تمرین ۱۳). بخصوص، D_4 مساوی (یکریخت) گروه D_4^* تقارنهای مربع است (ر.ک. صفحات ۳۸ تا ۳۹).

قضیهٔ ۸.۳ ؛ بازای هر $n \geq 3$ ، گروه دو وجهی D_n گروهی از مرتبهٔ $2n$ است که مولدهای a و b آن در روابط زیر صدق می‌کنند :

(یک) $a^n = (1)$ ؛ $b^2 = (1)$ ؛ اگر $0 < k < n$ ، $a^k \neq (1)$ ؛

(دو) $ba = a^{-1}b$.

هر گروه G تولید شده به وسیلهٔ عناصر $a,b \in G$ و صادق در (یک) و (دو) بازای $n \geq 3$ (با $e \in G$ بجای (1)) با D_n یکریخت است.

طرح برهان. تحقیق کنید که $a,b \in D_n$ به صورت تعریف شده در بالا در (یک) و (دو) صدق می‌کنند، و از آنجا $D_n = \langle a,b \rangle = \{a^i b^j \mid 0 \leq i < n;\ j = 0,1\}$ (ر.ک. قضیهٔ ۸.۲). سپس تحقیق کنید که $2n$ عنصر $a^i b^j$ $(0 \leq i < n; j = 0,1)$ همه متمایزند (فقط عملشان را بر 1 و 2 امتحان کنید)؛ درنتیجه، $|D_n| = 2n$.

فرض‌کنیم گروه G به‌وسیلهٔ $a,b \in G$ تولیدشده‌باشد و a,b بازای $n \geq 3$ ی در (یک) و (دو) صدق کنند. بنابر قضیهٔ ۸.۲ ، هر عنصر G حاصلضربی متناهی مانند $(m_i \in \mathbf{Z}) a^{m_1} b^{m_2} a^{m_3} b^{m_4} \cdots b^{m_k}$ است. با استفادهٔ مکرر از (یک) و (دو) ، هرچنین حاصلضرب را می‌توان به شکل $a^i b^j$ ، بازای $0 \leq i < n$ و $j = 0,1$ ، نوشت (بخصوص، توجه کنید که $b^2 = e$ و (دو) ایجاب می‌کند که $b = b^{-1}$ و $ab = ba^{-1}$). مولدهای D_n را با a_1, b_1 نشان دهید تا از ابهام جلوگیری کند و تحقیق کنید که نگاشت $f: D_n \to G$ داده شده با

$a_1^i b_1^j \to a^i b^j$ یک بروریختی گروههاست . برای اتمام برهان ، نشان می‌دهیم f یک تکریختی است . فرض کنیم $f(a_1^i b_1^i) = a^i b^i = e \in G$ با $0 \le i < n$ و $j = 0,1$. هرگاه $j = 1$ ، آنگاه $a^i = b$ و ، بنابر (دو) ، $a^{i+1} = a^i a = ba = a^{-1}b = a^{-1}a^i = a^{i-1}$ ، که ایجاب می‌کند که $a^2 = e$. این (یک) را نقض می‌کند ، زیرا $n \ge 3$. بنابراین ، $j = 0$ و $e = a^i b^0 = a^i$ با $0 \le i < n$ ، که بنابر (یک) $i = 0$ را ایجاب می‌کند . لذا ، $f(a_1^i b_1^i) = e$ ایجاب می‌کند که $a_1^i b_1^i = a_1^0 b_1^0 = (1)$. بنابراین ، طبق قضیهٔ ۳۰۲ ، f یک تکریختی است .

این قضیه مثالی است از مشخص کردن یک گروه برحسب "مولدها و روابط" . بحث مشروح این ایده در بخش ۹ داده خواهد شد .

تمرینات

۱ . چهار زیرگروه مختلف از S_4 بیابید که با S_3 یکریخت و نه زیرگروه بیابید که با S_2 یکریخت باشند .

۲ . (آ) S_n به وسیلهٔ $n-1$ ترانهش $(12), (13), (14), \ldots, (1n)$ تولید شده است . [**راهنمایی** . $(1i)(1j)(1i) = (ij)$.]

(ب) S_n به‌وسیلهٔ $n-1$ ترانهش $(12), (23), (34), \ldots, (n-1\ n)$ تولید شده است .

[**راهنمایی** . $(1j) = (1\ j-1)(j-1\ j)(1\ j-1)$ ؛ از (آ) استفاده کنید .]

۳ . هرگاه $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ و $\tau \in S_n$ ، آنگاه $\tau\sigma\tau^{-1}$ ، r- دور $(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$ است .

۴ . (آ) S_n با $\sigma_1 = (12)$ و $\tau = (123\cdots n)$ تولید شده است . [**راهنمایی** . تمرین ۳ را در مورد $\sigma_1, \sigma_2 = \tau\sigma_1\tau^{-1}, \sigma_3 = \tau\sigma_2\tau^{-1}, \ldots, \sigma_{n-1} = \tau\sigma_{n-2}\tau^{-1}$ به کار برده و از تمرین ۲ (ب) استفاده کنید .]

(ب) S_n به وسیلهٔ (12) و $(23\cdots n)$ تولید شده است .

۵ . فرض کنید $\sigma, \tau \in S_n$. هرگاه σ زوج (فرد) باشد ، آنگاه $\tau\sigma\tau^{-1}$ نیز چنین است .

۶ . A_n تنها زیرگروه S_n با اندیس 2 است . [**راهنمایی** . نشان دهید که هر زیرگروه با اندیس 2 باید شامل تمام 3- دورهای S_n باشد و لم ۱۱۰۶ را به‌کار برید .]

۷ . نشان دهید که $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ یک زیرگروه نرمال S_4 مشمول

A_4 است به‌طوری‌که $S_4/N \cong S_3$ و $A_4/N \cong Z_3$.

۸ . گروه A_4 زیرگروهی از مرتبهٔ 6 ندارد .

۹ . به‌ازای $n \geq 3$ ، فرض کنید G_n گروه ضربی ماتریسهای مختلطی باشد که به وسیلهٔ $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ و $y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$ تولید می‌شود ، که در آن $i^2 = -1$. نشان دهید که $G_n \cong D_n$. (**راهنمایی** . به یاد آورید که $e^{2\pi i} = 1$ و $e^{k2\pi i} \neq 1$ ، که در آن k حقیقی است ، مگر آنکه $k \in \mathbf{Z}$.)

۱۰ . فرض‌کنید a مولد D_n ازمرتبهٔ n باشد . نشان‌دهیدکه $\langle a \rangle \lhd D_n$ و $D_n/\langle a \rangle \cong Z_2$.

۱۱ . تمام زیرگروههای نرمال $\mathbf{D_n}$ را بیابید .

۱۲ . مرکز (تمرین ۱۱.۲) گروه D_n مساوی $\langle e \rangle$ است اگر n فرد باشد و با Z_2 یکریخت است اگر n زوج باشد .

۱۳ . به‌ازای‌هر $n \geq 3$ ، فرض کنید P_n یک n ضلعی منتظم باشد (به‌ازای $n = 3$ ، P_n مثلث متساوی‌الاضلاع است ؛ به‌ازای $n = 4$ ، مربع می‌باشد) . یک **تقارن** از P_n بیژکسیونی است مانند $P_n \to P_n$ که فواصل را حفظ‌کرده و رئوس مجاور را به رئوس مجاور می‌نگارد .

(آ) مجموعهٔ D_n^* مرکب از تمام تقارنهای P_n تحت عمل دوتایی ترکیب توابع یک گروه است .

(ب) هر $f \in D_n^*$ کاملا" با عملش بر رئوس P_n معین می‌شود . رئوس را متوالیا" شماره‌گذاری می‌کنیم : $1,2,\ldots,n$ ؛ دراین‌صورت ، هر $f \in D_n^*$ جایگشت منحصر به فردی مانند σ_f از $\{1,2,\ldots,n\}$ را معین می‌کند . ارتباط $f \mapsto \sigma_f$ یک تکریختی از گروهها را تعریف می‌کند : $\varphi : D_n^* \to S_n$.

(پ) D_n^* به‌وسیلهٔ f و g تولید می‌شود ، که در آن f دوران حول مرکز P_n به اندازهٔ $2\pi/n$ بوده و g انعکاس نسبت به "قطر" مار بر مرکز وراس 1 است .

(ت) $\sigma_f = (123\cdots n)$ و $\sigma_g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$ ، که از آنجا $Im\,\varphi = D_n$ و $D_n^* \cong D_n$.

۷ رسته‌ها : حاصلضربها ، هم‌حاصلضربها ، و اشیاء آزاد

اکنون که چند مثال در اختیار داریم ، وقتش رسیده که مفهوم رسته را معرفی کنیم . رسته

زبان سودمندی است و زمینه‌ای عمومی برای پرداختن به حالات مختلف ریاضی را فراهم می‌کند. این مفهوم به تفصیل در فصل ده مطالعه خواهد شد.

ایدهٔ شهودی در تعریف رسته این است که چند شیء ریاضی که قبلاً معرفی شده‌اند (مجموعه‌ها، گروهها، تکگونها) یا معرفی خواهند شد (حلقه‌ها، مدولها) همراه با نگاشتهای مناسبی از این اشیاء (توابع برای مجموعه‌ها؛ همریختیها برای گروهها، و غیره) از خواص صوری مشترکی برخوردارند. مثلاً، در هر حالت، ترکیب نگاشتها (وقتی تعریف شده‌اند) شرکتپذیر است؛ هر شیٔ A دارای نگاشت همانی $1_A : A \to A$ با خواص مشخصی است. این مفاهیم در تعریف زیرصوری شده‌اند.

تعریف ۱۰۷. هررسته‌رده‌ای‌است مانند $\mathcal{C}$ از اشیاء (که با $A,B,C,\ldots$ نموده می‌شوند) به انضمام

(یک) یک‌رده‌از مجموعه‌های از هم جدا، که با $hom(A,B)$ نموده می‌شود، برای هر جفت از اشیاء در $\mathcal{C}$ یکی (عنصر f از $hom(A,B)$ یک ریخت از A به B نامیده و با $f : A \to B$ نموده می‌شود)؛

(دو) به‌ازای هر سه تایی (A,B,C) از اشیاء در $\mathcal{C}$، تابعی مانند

$$hom(B,C) \times hom(A,B) \to hom(A,C)$$

(برای ریختهای $f : A \to B,\ g : B \to C$، این تابع به صورت $(g,f) \mapsto g \circ f$ نوشته و $g \circ f : A \to C$ ترکیب f و g خوانده می‌شود) که در دو اصل موضوع زیر صدق می‌کند:

(یک) شرکتپذیری. هرگاه $f : A \to B, g : B \to C, h : C \to D$ ریختهایی از $\mathcal{C}$ باشند، آنگاه $h \circ (g \circ f) = (h \circ g) \circ f$.

(دو) همانی. به‌ازای هر شیٔ B از $\mathcal{C}$، ریختی مانند $1_B : B \to B$ وجود دارد به‌طوری‌که به‌ازای هر $f : A \to B, g : B \to C$،

$$1_B \circ f = f \quad \text{و} \quad g \circ 1_B = g.$$

در رستهٔ $\mathcal{C}$، ریخت $f : A \to B$ را یک **تعادل** نامند اگر ریختی مانند $g : B \to A$ در $\mathcal{C}$ موجود باشد به‌طوری‌که $g \circ f = 1_A$ و $f \circ g = 1_B$. ترکیب دو تعادل، وقتی تعریف شده باشند، یک تعادل است. اگر $f : A \to B$ تعادل باشد، گویند A و B **معادل** می‌باشند.

مثال. فرض کنیم $\mathcal{S}$ ردهٔ تمام مجموعه‌ها باشد؛ به‌ازای $A,B \in \mathcal{S}$، $hom(A,B)$ مجموعهٔ

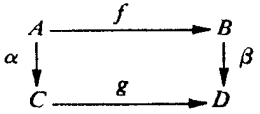
تمام توابع $f : A \to B$ است. به آسانی دیده می‌شود که $\mathcal{S}$ یک رسته است. طبق رابطهٔ (۱۳) در آشنایی، بخش ۳، ریخت f از $\mathcal{S}$ یک تعادل است اگر و فقط اگر f بیژکسیون باشد.

مثال. فرض کنیم $\mathcal{G}$ رسته‌ای باشد که اشیاء آن تمام گروهها می‌باشند؛ $\hom(A,B)$ مجموعهٔ تمام همریختیهای گروه $f : A \to B$ است. طبق قضیهٔ ۳۰۲، ریخت f یک تعادل است اگر و فقط اگر f یکریختی باشد. رستهٔ $\mathcal{A}$ مرکب از تمام گروههای آبلی به نحو مشابه تعریف می‌شود.

مثال. گروه (ضربی) G را می‌توان رسته‌ای با یک شیء، یعنی G، در نظر گرفت. فرض کنیم $\hom(G,G)$ مجموعهٔ تمام عناصر G باشد؛ ترکیب ریختهای a,b چیزی جز ترکیب ab با عمل دوتایی در G نیست. هر ریخت یک تعادل است (زیرا هر عنصر G معکوس دارد). 1_G عنصر همانی e از G است.

مثال. فرض کنیم اشیاء همه مجموعه‌های جزئی مرتب $(S,\leq)$ باشند. ریخت $(S,\leq) \to (T,\leq)$ تابعی است مانند $f : S \to T$ به‌طوری که به‌ازای $x,y \in S$، $x \leq y \Rightarrow f(x) \leq f(y)$.

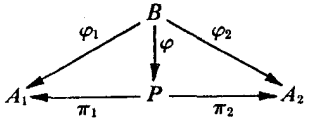
مثال. فرض کنیم $\mathcal{C}$ یک رسته بوده و اشیاء رستهٔ $\mathcal{D}$ تمام ریختهای $\mathcal{C}$ باشند. هرگاه $f : A \to B$ و $g : C \to D$ ریختهایی از $\mathcal{C}$ باشند، آنگاه $\hom(f,g)$ مرکب است از تمام جفتهای (α,β)، که در آن $\alpha : A \to C$, $\beta : B \to D$ ریختهایی از $\mathcal{C}$ اند به‌طوری‌که نمودار زیر تعویضپذیر است:



تعریف ۲۰۷. فرض کنیم $\mathcal{C}$ یک رسته بوده و $\{A_i \mid i \in I\}$ خانواده‌ای از اشیاء $\mathcal{C}$ باشد. یک *حاصلضرب* برای خانوادهٔ $\{A_i \mid i \in I\}$ شیئی است مانند P از $\mathcal{C}$ همراه با خانواده‌ای از ریختها مانند $\{\pi_i : P \to A_i \mid i \in I\}$ به‌طوری‌که به‌ازای هر شئ B و خانوادهٔ $\{\varphi_i : B \to A_i \mid i \in I\}$ از ریختها، ریخت منحصر به فردی مانند $\varphi : B \to P$ وجود دارد. به‌طوری‌که به‌ازای هر

$\pi_i \circ \varphi = \varphi_i$ ، $i \in I$.

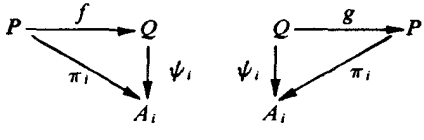
حاصلضرب P برای $\{A_i \mid i \in I\}$ معمولا "با $\prod_{i \in I} A_i$ نموده می‌شود . گاهی ، مخصوصا " در حالت $I = \{1,2\}$ ، توصیف حاصلضرب برحسب‌نمودارهای تعویضپذیر سودمند است . یک حاصلضرب بـرای $\{A_1, A_2\}$ نموداری است (از اشیاء و ریختها) مانند $A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2$ به‌طوری‌که به‌ازای هر نمودار دیگر به شکل $A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} A_2$ ، ریخت منحصر به فردی مانند $\varphi : B \to P$ هست به‌طوری‌که نمودار زیر تعویضپذیر می باشد:



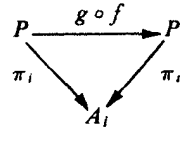
هرخانواده ازاشیاء در یک رسته لازم نیست حاصلضرب داشته باشد . اما ، در چند رستهٔ آشنا ، حـاصلضربها همواره وجود دارند . مثلا " ، بنابرآشنایی، قضیهٔ ۲۰۵ ، در رستهٔ مجموعه‌ها ، حاصلضرب دکارتی $\prod_{i \in I} A_i$ یک حاصلضرب برای خانوادهٔ $\{A_i \mid i \in I\}$ است . در بخش بعد ، نشان خواهیم داد که در رستهٔ گروهها حاصلضربها وجود دارند .

قضیهٔ ۳۰۷ . *هرگاه* $(P,\{\pi_i\})$ و $(Q,\{\psi_i\})$ *هردوحاصلضرب برای خانوادهٔ* $\{A_i \mid i \in I\}$ *از اشیاء رستهٔ* $\mathcal{C}$ *باشند ، آنگاه* P و Q *هم‌ارزند .*

برهان . چون P و Q هر دو حاصلضرب‌اند ، ریختهایی مانند $f : P \to Q$ و $g : Q \to P$ وجود دارند به‌طوری‌که نمودارهای زیر به‌ازای هر $i \in I$ تعویضپذیرند :



از ترکیب اینها به‌ازای هر $i \in I$ نمودار تعویضپذیر زیر به دست می‌آید :



لذا، $g \circ f : P \to P$ یک‌ریخت است به‌طوری‌که به‌ازای هر $i \in I$ ، $\pi_i \circ (g \circ f) = \pi_i$. اما، طبق‌تعریف حاصل‌ضرب، ریخت منحصر به فردی با این خاصیت وجود دارد. چون نگاشت $1_P : P \to P$ نیزطوری است‌که به‌ازای هر $i \in I$ ، $\pi_i \circ 1_P = \pi_i$ ، طبق یکتایی، باید داشته باشیم $g \circ f = 1_P$. به همین نحو، با استفاده از حاصل‌ضرب بودن Q ، می‌توان نشان داد که $f \circ g = 1_Q$. ازاینرو، $f : P \to Q$ یک تعادل است.

چون رسته‌های مجرد فقط شامل اشیاء و ریختها هستند (بدون عنصر)، هر حکم در باب آنها حکمی دوگان دارد که از معکوس کردن تمام سهمها (ریختها) در حکم اصلی به دست می‌آید. مثلا"، دوگان تعریف ۲۰۷ عبارت است از

تعریف ۴۰۷ . یک **هم‌حاصل‌ضرب** (یا **مجموع**) برای خانوادهٔ $\{A_i \mid i \in I\}$ از اشیاء در رستهٔ $\mathcal{C}$ شیئ S است‌مانند S از $\mathcal{C}$ ، همراه‌باخانواده‌ای‌ازریختها مانند $\{\iota_i : A_i \to S \mid i \in I\}$ ، به‌طوری‌که به‌ازای هر شیئ B و خانوادهٔ $\{\psi_i : A_i \to B \mid i \in I\}$ از ریختها، ریخت منحصر به فردی مانند $\psi : S \to B$ موجود باشد به‌طوری‌که به‌ازای هر $i \in I$ ، $\psi \circ \iota_i = \psi_i$.

اگرچه گاهی $\coprod_{i \in I} A_i$ به کار می‌رود، اما نماد یکنواختی برای هم‌حاصل‌ضرب وجود ندارد.

در دوبخش آتی هم‌حاصل‌ضربها را در رستهٔ $\mathcal{G}$ گروهها و رستهٔ $\mathcal{A}$ گروههای آبلی مطرح خواهیم کرد. قضیهٔ زیر را می‌توان با استفاده از" برهان دوگان "برهانی‌که در اثبات قضیهٔ ۳۰۷ به کار رفت اثبات کرد (ثابت کنید!).

قضیهٔ ۵۰۷ . *هرگاه* $(S, \{\iota_i\})$ و $(S', \{\lambda_i\})$ *هر دو هم‌حاصل‌ضربهایی برای خانوادهٔ* $\{A_i \mid i \in I\}$ *از اشیاء رستهٔ* $\mathcal{C}$ *باشند، آنگاه* S و S' *معادلند.*

در چند رستهٔ ذکر شده در بالا(مثلا"، گروهها)، هر شیئ در رسته‌در واقع مجموعه است (معمولا" با ساختاری اضافی) و هر ریخت $f : A \to B$ در رسته تابعی است بر "مجموعه‌های زمینه" (معمولا" همراه با خواصی دیگر). این ایده را صوری می‌سازیم.

تعریف ۶.۷ . رستهٔ ملموس رسته‌ای است مانند $\mathcal{C}$ همراه با تابعی چون σ که به هر شیٔ A از $\mathcal{C}$ مجموعهٔ $\sigma(A)$ (به نام مجموعهٔ زمینهٔ A) را نسبت می‌دهد به‌طوری‌که
(یک) هر ریخت $A \to B$ از $\mathcal{C}$ تابعی بر مجموعه‌های زمینهٔ $\sigma(A) \to \sigma(B)$ است؛
(دو) ریخت همانی هر شیٔ A از $\mathcal{C}$ تابع همانی بر مجموعهٔ زمینهٔ $\sigma(A)$ است؛
(سه) ترکیب ریختها در $\mathcal{C}$ با ترکیب توابع بر مجموعه‌های زمینه یکی است.

چند مثال. رستهٔ گروهها مجهز به تابعی که به هر گروه مجموعهٔ زمینه‌اش در معنی عادی را نسبت می‌دهد یک رستهٔ ملموس است. به همین نحو، رسته‌های گروههای آبلی و مجموعه‌های جزئی مرتب، با مجموعه‌های زمینهٔ واضح، رسته‌هایی ملموس‌اند. لیکن، در مثال سوم بعد از تعریف ۱.۷، هرگاه تابع σ به گروه G مجموعهٔ زمینهٔ معمولی G را نسبت دهد، آنگاه رستهٔ مورد بحث ملموس نیست (زیرا ریختها بر مجموعهٔ G تابع نیستند).

رسته‌های ملموس بارها مفید واقع می‌شوند، زیرا نه تنها خواص رسته را دارند، بلکه بعضی از خواص مجموعه‌ها، زیرمجموعه‌ها، وغیره را نیز دارا می‌باشند. چون در هر رستهٔ ملموس اساساً به تابع σ که به یک شیٔ مجموعهٔ زمینه‌اش در معنی عادی را نسبت می‌دهد (مثل مثالهای فوق) توجه داریم، شیٔ و مجموعهٔ زمینه را با یک علامت نشان داده و از ذکر صریح σ خودداری می‌کنیم. امکان ابهام کمی وجود دارد، زیرا در رستهٔ ملموس $\mathcal{C}$ مواظبیم که بین *ریختهای* $\mathcal{C}$ (که، طبق تعریف، بر مجموعه‌های زمینه تابع نیز هستند) و *نگاشتها* (توابع بر مجموعه‌های زمینه، که ممکن است ریختهایی از $\mathcal{C}$ نباشند) تمایز قایل شویم.

تعریف ۷.۷ . فرض کنیم F شیٔ در رستهٔ ملموس $\mathcal{C}$، X مجموعه‌ای ناتهی، و $i : X \to F$ یک نگاشت (از مجموعه‌ها) باشد. F بر مجموعهٔ X *آزاد* است اگر به ازای هر شیٔ A از $\mathcal{C}$ و نگاشت (از مجموعه‌های) $f : X \to A$، ریخت منحصر به فردی از $\mathcal{C}$ مانند $\bar{f} : F \to A$ موجود باشد به‌طوری‌که، (به عنوان تابعی از مجموعه‌های $X \to A$) $\bar{f}i = f$.

نکتهٔ مهم در باب شیٔ آزاد F این است که *برای تعریف یک ریخت با دامنهٔ F کافی است نقش زیرمجموعهٔ $i(X)$ به صورت دیده شده در مثالهای زیر مشخص شود.*

چند مثال. فرض کنیم G گروه و $g \in G$. به آسانی دیده می‌شود که نگاشت $\bar{f}: \mathbf{Z} \to G$ تعریف شده با $\bar{f}(n) = g^n$ همریختی منحصر به فردی است مانند $\mathbf{Z} \to G$ به طوری‌که $1 \mapsto g$. درنتیجه، هرگاه $X = \{1\}$ و $i: X \to \mathbf{Z}$ نگاشت شمول باشد، آنگاه $\mathbf{Z}$ بر X در رسته‌ٔ گروهها آزاد است (اگر $f: X \to G$ ، فرض می‌کنیم $g = f(1)$ و $\bar{f}$ را مثل بالا تعریف می‌کنیم). به عبارت دیگر، برای تعیین همریختی منحصر به فرد از $\mathbf{Z}$ به G ، فقط کافی است نقش $1 \in \mathbf{Z}$ (یعنی، نقش $i(X)$) را مشخص کنیم. گروه (جمعی) $\mathbf{Q}$ از اعداد گویا این خاصیت را **ندارد**. اثبات اینکه همریختی نابدیهی $\mathbf{Q} \to S_3$ وجود ندارد مشکل نیست. لذا، به ازای هر مجموعه‌ٔ X ، تابع $i: X \to \mathbf{Q}$ و تابع $f: X \to S_3$ که به‌ازای $x_1 \in X$ ی $f(x_1) \neq (1)$ ، همریختی مانند $\bar{f}: \mathbf{Q} \to S_3$ با خاصیت $\bar{f}i = f$ وجود ندارد.

قضیه‌ٔ ۸.۶. *هرگاه $\mathfrak{C}$ یک رسته‌ٔ ملموس، F و F' اشیائی از $\mathfrak{C}$ باشند به‌طوری‌که F بر مجموعه‌ٔ X و F' بر مجموعه‌ٔ X' آزاد باشد، و نیز $|X| = |X'|$ ، آنگاه F با F' معادل است.*

توجه کنید که مفروضات وقتی برقرارند که F و F' هردو بر یک مجموعه‌ٔ X آزاد باشند.

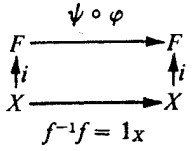
برهان ۸.۷. چون F, F' آزادند و $|X| = |X'|$ ، بیژکسیونی مانند $f: X \to X'$ و نگاشتهایی چون $i: X \to F$ و $j: X' \to F'$ وجود دارند. نگاشت $jf: X \to F'$ را در نظر می‌گیریم. چون F آزاد است، یک ریخت مانند $\varphi: F \to F'$ وجود دارد به‌طوری‌که نمودار

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & F' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ X & \xrightarrow[f]{} & X' \end{array}$$

تعویض‌پذیر است. به همین نحو، چون بیژکسیون f دارای معکوس $f^{-1}: X' \to X$ بوده و F' آزاد است، یک‌ریخت مانند $\psi: F' \to F$ وجود دارد به‌طوری‌که

$$\begin{array}{ccc} F' & \xrightarrow{\psi} & F \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle i} \\ X' & \xrightarrow[f^{-1}]{} & X \end{array}$$

تعویضپذیر است . از تلفیق این نمودارها نمودار تعویضپذیر زیر به دست می‌آید:



از اینرو ، $(\psi \circ \varphi)i = i1_X = i$. اما $1_F i = i$. لذا ، طبق خاصیت یکتایی اشیاء آزاد ، باید داشته باشیم $\psi \circ \varphi = 1_F$. استدلال مشابه نشان می‌دهد که $\varphi \circ \psi = 1_{F'}$. بنابراین ، F با F' هم‌ارز است .

حاصل‌ضربها ، هم‌حاصل‌ضربها ، و اشیاء آزاد همه به وسیلهٔ **خواص نگاشت عمومی** (یعنی ، برحسب وجود بعضی از ریختهای منحصر به فرد) تعریف شده‌اند . همچنین ، دیدیم که در واقع هر دو حاصل‌ضرب (یا هم‌حاصل‌ضرب) برای یک خانواده از اشیاء هم‌ارزند (قضیهٔ ۸۰۷) . به‌علاوه ، تشابه آشکاری بین برهانهای قضایای ۳۰۷ و ۸۰۷ وجود دارد . درنتیجه ، تعجب‌آور نیست که تمام مفاهیمی که هم‌اکنون ذکر شد حالات خاصی از یک مفهوم باشند .

تعریف ۹۰۷ . شیٔ I در رستهٔ $\mathcal{C}$ را **عمومی** (یا **اولیه**) گویند اگر به‌ازای هر شیٔ C از $\mathcal{C}$ ، یک و فقط یک ریخت مانند $I \to C$ موجود باشد . شیٔ T از $\mathcal{C}$ را **هم عمومی** (یا **نهایی**) گویند اگر به‌ازای هر شیٔ C از $\mathcal{C}$ ، یک و فقط یک ریخت مانند $C \to T$ وجود داشته باشد .

ذیلا " نشان خواهیم داد که حاصل‌ضربها ، هم حاصل‌ضربها ، و اشیاء آزاد را می‌توان اشیاء (هم) عمومی در رسته‌هایی مناسب در نظر گرفت . اما این مشخص سازی در آینده به‌کار نمی‌آید . چون اشیاء عمومی تا بخشهای ۴۰ III ، ۵۰ III ، و ۵۰ IV (جز گاهی در تمرینات) ذکر نمی‌شوند ، خواننده ممکن است فعلا " مطالب زیر را حذف نماید .

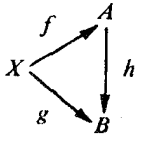
قضیهٔ ۱۰۰۷ . *هر دو شیٔ عمومی [یا هم عمومی] در رستهٔ $\mathcal{C}$ معادلند .*

برهان . فرض کنیم I و J اشیایی عمومی در $\mathcal{C}$ باشند . چون I عمومی است ، ریخت

منحصربه‌فردی مانند $f: I \to J$ وجود دارد. به همین نحو، چون J عمومی است، ریخت منحصربه‌فردی مانند $g: J \to I$ وجود دارد. ترکیب $g \circ f: I \to I$ یک ریخت از $\mathcal{C}$ است. اما $1_I: I \to I$ نیز یک ریخت از $\mathcal{C}$ است. عمومیت I ایجاب می‌کند که ریخت منحصر به فردی مانند $I \to I$ وجود داشته باشد، که از آنجا $g \circ f = 1_I$. به همین نحو، عمومیت J ایجاب می‌کند که $f \circ g = 1_J$. بنابراین، $f: I \to J$ یک تعادل است. اثبات برای اشیاء هم عمومی به‌همین‌نحو است.

مثال. گروه بدیهی $\langle e \rangle$ در رستهٔ گروهها عمومی و هم عمومی است.

مثال. فرض کنیم F یک شیء آزاد بر مجموعهٔ X (با $i: X \to F$) در رستهٔ ملموس $\mathcal{C}$ باشد. رستهٔ جدید $\mathcal{D}$ را به صورت زیر تعریف می‌کنیم. اشیاء $\mathcal{D}$ همه نگاشتهایی از مجموعه‌ها مانند $f: X \to A$ اند، که A (مجموعهٔ زمینهٔ) یک شیء از $\mathcal{C}$ است. یک ریخت در $\mathcal{D}$ از $f: X \to A$ به $g: X \to B$ ریختی مانند $h: A \to B$ از $\mathcal{C}$ تعریف می‌شود به‌طوری‌که نمودار



تعویضپذیر است (یعنی، $hf = g$). تحقیق کنید که $1_A: A \to A$ ریخت همانی از f به f در $\mathcal{D}$ بوده و h یک تعادل در $\mathcal{D}$ است اگر و فقط اگر h یک تعادل در $\mathcal{C}$ باشد. چون F بر مجموعهٔ X آزاد است، به‌ازای هر نگاشت $f: X \to A$ ریخت منحصر به فردی مانند $\bar{f}: F \to A$ وجود دارد به‌طوری‌که $\bar{f}i = f$. این دقیقاً" یعنی $i: X \to F$ یک شیء عمومی در رستهٔ $\mathcal{D}$ است.

مثال. فرض کنیم $\{A_i \mid i \in I\}$ خانواده‌ای از اشیاء در رستهٔ $\mathcal{C}$ باشد. رستهٔ $\mathcal{E}$ طوری است که اشیاء آن تمام جفتهای $(B, \{f_i \mid i \in I\})$ اند، که B شیء از $\mathcal{C}$ بوده و به‌ازای هر i، $f_i: B \to A_i$ یک ریخت از $\mathcal{C}$ است. یک ریخت در $\mathcal{E}$ از $(B, \{f_i \mid i \in I\})$ به $(D, \{g_i \mid i \in I\})$ ریختی مانند $h: B \to D$ از $\mathcal{C}$ تعریف می‌شود به‌طوری‌که به‌ازای هر $i \in I$، $g_i \circ h = f_i$.

تحقیق کنید که 1_B ریخت همانی از $(B,\{f_i\})$ به $(B,\{f_i\})$ در $\mathcal{E}$ بوده و h یک تعادل در $\mathcal{E}$ است اگر و فقط اگر h یک تعادل در $\mathcal{C}$ باشد. هرگاه در $\mathcal{C}$ حاصلضربی برای خانوادهٔ $\{A_i \mid i \in I\}$ (با نگاشتهای $\pi_k : \prod A_i \to A_k$ به‌ازای هر $k \in I$) وجود داشته باشد، آنگاه به‌ازای هر $i \in I$ ، $\pi_i \circ f = f_i$. اما این می‌گوید که $(\prod A_i, \{\pi_i \mid i \in I\})$ یک شیٔ هم عمومی در رستهٔ $\mathcal{E}$ است. به همین نحو، هم حاصلضرب خانواده‌ای از اشیاء در $\mathcal{C}$ را می‌توان یک شیٔ عمومی در رسته‌ای مناسب در نظر گرفت.

چون حاصلضرب $\prod A_i$ برای خانوادهٔ $\{A_i \mid i \in I\}$ در یک رسته را می‌توان یک شیٔ هم عمومی در رسته‌ای مناسب گرفت، از قضیهٔ ۱۰.۷ فوراً نتیجه می‌شود که $\prod A_i$ به طور منحصر به فرد با تقریب تعادل معین می‌شود. نتایج مشابهی برای حاصلضربها و اشیاء آزاد برقرارند.

تمرینات

۱. یک **مجموعهٔ نقطه‌ای** جفتی مانند (S,x) است که در آن S مجموعه است و $x \in S$. یک ریخت از مجموعه‌های نقطه‌ای مانند $(S,x) \to (S',x')$ سه‌تایی است مانند (f,x,x')، که در آن $f : S \to S'$ تابعی است که $f(x) = x'$. نشان دهید که مجموعه‌های نقطه‌ای رسته تشکیل می‌دهند.

۲. اگر $f : A \to B$ یک تعادل در رستهٔ $\mathcal{C}$ بوده و $g : B \to A$ یک ریخت باشد به‌طوری که $g \circ f = 1_A, f \circ g = 1_B$، نشان دهید که g منحصر به فرد است.

۳. در رستهٔ $\mathcal{G}$ از گروهها، نشان دهید که گروه $G_1 \times G_2$ همراه با همریختیهای $\pi_1 : G_1 \times G_2 \to G_1$ و $\pi_2 : G_1 \times G_2 \to G_2$ (مثل مثال قبل از تعریف ۲.۲) حاصلضربی برای $\{G_1,G_2\}$ است.

۴. در رستهٔ $\mathcal{A}$ از گروههای آبلی، نشان دهید که گروه $A_1 \times A_2$ همراه با همریختیهای $\iota_1 : A_1 \to A_1 \times A_2$ و $\iota_2 : A_2 \to A_1 \times A_2$ (مثل مثال قبل از تعریف ۲.۲) یک هم حاصلضرب برای $\{A_1,A_2\}$ است.

۵. هر خانوادهٔ $\{A_i \mid i \in I\}$ در رستهٔ مجموعه‌ها دارای هم حاصلضرب است. [**راهنمایی.** $\bigcup A_i = \{(a,i) \in (\bigcup A_i) \times I \mid a \in A_i\}$ را در نظر می‌گیریم که $a \mapsto (a,i)$ با $A_i \to \bigcup A_i$ داده شده است. $\bigcup A_i$ را *اجتماع از هم جدای* مجموعه‌های A_i می‌نامند.]

۶ . (آ) نشان دهید که در رستهٔ $\mathbf{s}_*$ از مجموعه‌های نقطه‌ای (ر.ک. تمرین ۱) حاصل ضربها همیشه وجود دارند، آنها را توصیف کنید.

(ب) نشان دهید که هر خانواده در $\mathbf{s}_*$ دارای هم حاصلضرب است (که اغلب یک "حاصلضرب فشار" نامیده می‌شود)؛ این هم حاصلضرب را توصیف کنید.

۷ . فرض کنید F یک شیء آزاد بر مجموعهٔ X $(i: X \to F)$ در رستهٔ ملموس $\mathcal{C}$ باشد. هرگاه $\mathcal{C}$ حاوی شیء باشد که مجموعهٔ زمینه‌اش دست کم دو عنصر در آن دارد، آنگاه i یک نگاشت انژکتیو از مجموعه‌ها است.

۸ . فرض کنید X یک مجموعه و F یک شیء آزاد بر X (با $i: X \to F$) در رستهٔ گروهها باشد (وجود F در بخش ۹ ثابت شده است). ثابت کنید $i(X)$ مجموعه‌ای از مولدها برای گروه F است. [**راهنمایی.** هرگاه G زیرگروه F و تولید شده به وسیلهٔ $i(X)$ باشد، آنگاه یک همریختی مانند $\varphi: F \to G$ هست به طوری که $\varphi i = i$. نشان دهید که $F \xrightarrow{\varphi} G \subseteq F$ نگاشت همانی است.]

۸ حاصلضربهای مستقیم و مجموعهای مستقیم

در این بخش حاصل ضربها در رستهٔ گروهها و هم حاصلضربها در رستهٔ گروههای آبلی را مطالعه می‌کنیم. این حاصلضربها و هم حاصلضربها نه تنها ابزاری برای ساختن گروههای جدید از قدیمند، بلکه برای توصیف ساختار بعضی از گروهها برحسب زیرگروههای خاص (که، مثلا"، ساختارشان از قبل معلوم است) نیز به کار می‌روند.

بحث را با تعمیم تعریف حاصلضرب مستقیم $G \times H$ گروههای G و H (ر.ک. صفحهٔ ۴۰) به خانواده‌ای از گروههای دلخواه (احتمالا" نامتناهی) از گروههای $\{G_i \mid i \in I\}$ آغاز می‌کنیم. برحاصلضرب دکارتی $\coprod_{i \in I} G_i$ (از مجموعه‌ها) یک رابطهٔ دوتایی به صورت زیر تعریف می‌کنیم:

هرگاه $f, g \in \prod_{i \in I} G_i$ (یعنی، $f, g: I \to \bigcup_{i \in I} G_i$ و، به ازای i، $f(i), g(i) \in G_i$)، آنگاه $fg: I \to \bigcup_{i \in I} G_i$ تابعی است که با $i \to f(i)g(i)$ داده می‌شود. چون هر G_i گروه است، به ازای هر i، $f(i)g(i) \in G_i$، که از آنجا، بنابر آشنایی، تعریف ۱۰۵، $fg \in \prod_{i \in I} G_i$.

هرگاه $f \in \prod_{i \in I} G_i$ را با نقشش $\{a_i\}$ (به ازای هر $i \in I$، $a_i = f(i)$) یکی کنیم، که معمولا"

وقتی I متناهی است انجام می‌شود ، آنگاه عمل دوتایی در $\prod_{i\in I} G_i$ ضرب مؤلفه به مؤلفهٔ آشنا می‌باشد : $\{a_i\}\{b_i\}=\{a_ib_i\}$. $\prod_{i\in I} G_i$ ، همراه با این عمل دوتایی ، یک *حاصل‌ضرب مستقیم* (یا *مجموع مستقیم تام*) برای خانوادهٔ $\{G_i \mid i\in I\}$ از گروهها نامیده می‌شود . اگر $I=\{1,2,\ldots,n\}$ ، $\prod_{i\in I} G_i$ را معمولاً با $G_1\times G_2\times\cdots\times G_n$ (یا ، در نماد جمعی ، با $G_1\oplus G_2\oplus\cdots\oplus G_n$) نشان می‌دهند .

قضیهٔ ۱۰۸ . *هرگاه $\{G_i \mid i\in I\}$ خانواده‌ای از گروهها باشد ، آنگاه*
(یک) حاصل‌ضرب مستقیم $\prod_{i\in I} G_i$ یک گروه است ؛
(دو) به‌ازای هر $k\in I$ ، نگاشت $\pi_k:\prod_{i\in I} G_i\to G_k$ داده‌شده با $f\mapsto f(k)$ [یا $\{a_i\}\mapsto a_k$] یک برووریختی گروهها است .

برهان . تمرین .

نگاشتهای π_k در قضیهٔ ۱۰۸ *تصویرهای کانونی* حاصل‌ضرب مستقیم نامیده می‌شوند .

قضیهٔ ۲۰۸ . *فرض کنیم $\{G_i \mid i\in I\}$ خانواده‌ای از گروهها بوده و $\{\varphi_i:H\to G_i \mid i\in I\}$ خانواده‌ای از همریختیهای گروهها باشد . در این صورت ، همریختی منحصر به فردی مانند $\varphi:H\to\prod_{i\in I} G_i$ هست به‌طوری‌که به‌ازای هر $i\in I$ ، $\pi_i\varphi=\varphi_i$ و این خاصیت $\prod_{i\in I} G_i$ را با تقریت یکریختی معین می‌کند . به عبارت دیگر ، $\prod_{i\in I} G_i$ یک حاصل‌ضرب در رستهٔ گروهها است.*

برهان . بنابر آشنایی ، قضیهٔ ۲۰۵ ، نگاشت مجموعه‌های $\varphi:H\to\prod_{i\in I} G_i$ داده شده با $\varphi(a)=\{\varphi_i(a)\}_{i\in I}\in\prod_{i\in I} G_i$ تابع منحصر به فردی است به‌طوری‌که به‌ازای هر $i\in I$ ، $\pi_i\varphi=\varphi_i$. به آسانی تحقیق می‌شود که φ یک همریختی است . از اینرو ، $\prod_{i\in I} G_i$ یک حاصل‌ضرب است (به معنی رسته‌ای) ؛ و لذا ، طبق قضیهٔ ۳۰۷ ، با تقریب (تعادل)

یکریختی معین است .

چون حاصلضرب مستقیم گروههای آبلی به وضوح آبلی است ، نتیجه می‌شود که حاصلضرب مستقیم گروههای آبلی حاصلضربی در رستهٔ گروههای آبلی نیز هست .

تعریف ۳۰۸ . *حاصلضرب مستقیم ضعیف (خارجی)* خانوادهٔ $\{G_i \mid i \in I\}$ از گروهها ، که با $\prod_{i\in I}^{w} G_i$ نموده می‌شود ، مجموعهٔ تمام $f \in \prod_{i\in I} G_i$ هایی است به‌طوری‌که به‌ازای هر $i \in I$ جز تعدادی متناهی ، (همانی در G_i) $f(i) = e_i$. اگر گروههای G_i همه آبلی (جمعی) باشند ، $\prod_{i\in I}^{w} G_i$ را معمولا " *مجموع مستقیم (خارجی)* نامیده و با $\sum_{i\in I} G_i$ نشان می‌دهند .

اگر I متناهی باشد ، حاصلضرب مستقیم ضعیف با حاصلضرب مستقیم یکی است . در هرحال ، داریم

قضیهٔ ۴۰۸ . *هرگاه $\{G_i \mid i \in I\}$ خانواده‌ای از گروهها باشد ، آنگاه*
(یک) $\prod_{i\in I}^{w} G_i$ زیرگروه نرمالی از $\prod_{i\in I} G_i$ است ؛
(دو) به‌ازای هر $k \in I$ ، نگاشت $\iota_k : G_k \to \prod_{i\in I}^{w} G_i$ داده شده با $\iota_k(a) = \{a_i\}_{i\in I}$ ، که در آن به‌ازای $i \neq k$ ، $a_i = e$ و $a_k = a$ ، یک تکریختی گروههاست ؛
(سه) به‌ازای هر $i \in I$ ، $\iota_i(G_i)$ یک زیرگروه نرمال $\prod_{i\in I} G_i$ است .

برهان . تمرین .

نگاشتهای ι_k در قضیهٔ ۴۰۸ *انژکسیونهای کانونی* نام دارند .

قضیهٔ ۵۰۸ . *فرض کنیم $\{A_i \mid i \in I\}$ خانواده‌ای از گروههای آبلی باشد (که جمعی نوشته می‌شوند) . هرگاه B گروهی آبلی بوده و $\{\psi_i : A_i \to B \mid i \in I\}$ خانواده‌ای از همریختیها باشد ، آنگاه همریختی منحصر به فردی مانند $\psi : \sum_{i\in I} A_i \to B$ هست به‌طوری‌که به‌ازای هر $i \in I$ ،*

$\psi\iota_i = \psi_i$ و این خاصیت $\sum_{i\in I} A_i$ را با تقریب یکریختی مشخص می‌کند. به عبارت دیگر، $\sum_{i\in I} A_i$ یک هم‌حاصل‌ضرب در رستهٔ گروههای آبلی است.

تبصره. قضیه در صورت حذف کلمهٔ آبلی درست نیست. حاصل‌ضرب مستقیم ضعیف خارجی در رستهٔ تمام گروهها یک هم‌حاصل‌ضرب نیست (تمرین ۴).

برهان ۵.۸. در سراسر این برهان تمام گروهها جمعی نوشته می‌شوند. هرگاه $\{a_i\} \in \sum A_i$ ، $\{a_i\} \neq 0$ ، آنگاه تنها تعدادی متناهی از a_i ها، مثلاً $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ ، ناصفرند. $\psi : \sum A_i \to B$ را با $\psi\{0\} = 0$ و $\psi(\{a_i\}) = \psi_{i_1}(a_{i_1}) + \psi_{i_2}(a_{i_2}) + \cdots + \psi_{i_r}(a_{i_r}) = \sum_{i\in I_0} \psi_i(a_i)$ تعریف می‌کنیم، که در آن I_0 مجموعهٔ $\{i_1, i_2, \ldots, i_r\} = \{i \in I \mid a_i \neq 0\}$ است. چون B آبلی است. فورا" تحقیق می‌شود که ψ یک همریختی است و به‌ازای هر $i \in I$ ، $\psi\iota_i = \psi_i$. به ازای هر $\{a_i\} \in \sum A_i$ ، $\{a_i\} = \sum_{i\in I_0} \iota_i(a_i)$ ، I_0 مثل بالا متناهی است. هرگاه $\xi : \sum A_i \to B$ یک همریختی باشد به‌طوری‌که به‌ازای هر i ، $\xi\iota_i = \psi_i$ ، آنگاه

$$\xi(\{a_i\}) = \xi(\sum_{I_0} \iota_i(a)) = \sum_{I_0} \xi\iota_i(a_i) = \sum_{I_0} \psi_i(a_i) = \sum_{I_0} \psi\iota_i(a_i) = \psi(\sum_{I_0} \iota_i(a_i)) = \psi(\{a_i\});$$

از اینرو، $\psi = \xi$ و ψ منحصر به فرد است. بنابراین، $\sum A_i$ در رستهٔ گروههای آبلی هم حاصل ضرب است، و درنتیجه، بنابر قضیهٔ ۵.۷، با تقریب (تعادل) یکریختی معین است.

حال شرایطی را بررسی می‌کنیم که تحت آنها گروه G با حاصل‌ضرب مستقیم ضعیف خانواده‌ای از زیرگروههایش یکریخت باشد.

قضیهٔ ۶.۸. فرض کنیم $\{N_i \mid i \in I\}$ خانواده‌ای از زیرگروههای نرمال گروه G باشد به‌طوری که

(یک) $G = \langle \bigcup_{i\in I} N_i \rangle$ ؛

(دو) به‌ازای هر $k \in I$ ، $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$.

در این صورت ، $G \cong \coprod_{i\in I}^{w} N_i$.

پیش از اثبات قضیه به حالت خاصی که مکرر به کار می‌رود توجه می‌کنیم : ملاحظه می‌کنیم که ، طبق تعمیم قضیهٔ ۳۰۵ که به آسانی ثابت می‌شود ، به‌ازای زیرگروههای نرمال $N_1, N_2, \ldots, N_r$ از گروه G ،

$$\langle N_1 \cup N_2 \cup \cdots \cup N_r \rangle = N_1 N_2 \cdots N_r = \{n_1 n_2 \cdots n_r \mid n_i \in N_i\} .$$

با نماد جمعی ، $N_1 N_2 \cdots N_r$ نوشته می‌شود $N_1 + N_2 + \cdots + N_r$. ممکن است به خاطر داشتن نتیجهٔ زیر برای خواننده مفید باشد ، زیرا برهان حالت کلی اساساً " همین است .

نتیجهٔ ۷۰۸ . *هرگاه* $N_1, N_2, \ldots, N_r$ *زیرگروههای نرمالی از گروه* G *باشند به طوری که* $G = N_1 N_2 \cdots N_r$ *و به‌ازای هر* $1 \le k \le r$ ، $N_k \cap (N_1 \cdots N_{k-1} N_{k+1} \cdots N_r) = \langle e \rangle$ ، *آنگاه* $G \cong N_1 \times N_2 \times \cdots \times N_r$.

برهان قضیهٔ ۶۰۸ . هرگاه $\{a_i\} \in \coprod^{w} N_i$ ، آنگاه به‌ازای هر $i \in I$ جز تعدادی متناهی $a_i = e$. فرض کنیم I_0 مجموعهٔ متناهی $\{i \in I \mid a_i \neq e\}$ باشد . در این صورت ، $\coprod_{i\in I_0} a_i$ عنصر تعریف شده‌ای از G است ، زیرا ، بنابر قضیهٔ ۳۰۵ (چهار) ، به‌ازای $a \in N_i$ و $b \in N_j$ $(i \neq j)$ ، $ab = ba$. درنتیجه ، نگاشت $\varphi : \coprod^{w} N_i \to G$ داده‌شده با $\{a_i\} \mapsto \coprod_{i\in I_0} a_i \in G$ (و $\{e\} \to e$) یک همریختی است به‌طوری‌که به‌ازای $a_i \in N_i$ ، $\varphi\iota_i(a_i) = a_i$.

چون G به‌وسیلهٔ زیرگروههای N_i تولید می‌شود ، هر عنصر a از G یک حاصلضرب متناهی از عناصر N_i های مختلف است . چون عناصر N_i و N_j (به‌ازای $i \neq j$) با هم تعویض می‌شوند ، a را می‌توان به صورت حاصلضرب $\coprod_{i\in I_0} a_i$ نوشت ، که در آن $a_i \in N_i$ و I_0 زیرمجموعه‌ای متناهی از I است . از اینرو ، داریم $\coprod_{i\in I_0} \iota_i(a_i) \in \coprod^{w} N_i$ و

$$\varphi(\coprod_{i\in I_0} \iota_i(a_i)) = \coprod_{i\in I_0} \varphi\iota_i(a_i) = \coprod_{i\in I_0} a_i = a$$

بنابراین ، φ یک‌بر و ریختی است .

فرض کنیم $\varphi(\{a_i\}) = \coprod_{i\in I_0} a_i = e \in G$. واضح است که می‌توان برای راحتی در نمادگذاری فرض کرد که $I_0 = \{1, 2, \ldots, n\}$. در این صورت ، $\coprod_{i\in I_0} a_i = a_1 a_2 \cdots a_n = e$ ، که در آن

$a_i \in N_i$. از اینرو، $a_1^{-1} = a_2 \cdots a_n \in N_1 \cap \langle \bigcup_{i \neq 1} N_i \rangle = \langle e \rangle$ ؛ ولـذا، $a_1 = e$. تکرار این استدلال نشان می‌دهد که به‌ازای هر $i \in I$ ، $a_i = e$. از اینرو، φ یک تکریختی است.

قضیهٔ ۶.۸ تعریف زیر را موجب می‌شود.

تعریف ۸.۸ . فرض کنیم $\{N_i \mid i \in I\}$ خانـواده‌ای از زیـرگروههای نرمال گروه G باشد به‌طوری‌کـه $\langle \bigcup_{i \in I} N_i \rangle = G$ و بـه‌ازای هر $k \in I$ ، $N_k \cap \langle \bigcup_{i \neq k} N_i \rangle = \langle e \rangle$. در این صورت، گوییم G *حاصل‌ضرب مستقیم ضعیف داخلی* خانوادهٔ $\{N_i \mid i \in I\}$ (یا *مجموع مستقیم داخلی* اگر G آبلی (جمعی) باشد) است.

به عنوان نتیجـهٔ آسـانی از قضیهٔ ۶.۸ ، توصیف زیر از حاصل ضربهای مستقیم ضعیف داخلی را داریم.

قضیهٔ ۹.۸ . *فرض کنیم $\{N_i \mid i \in I\}$ خانواده‌ای از زیرگروههای نرمال گروه G باشد. G حاصل‌ضرب مستقیـم ضعیف داخلـی خـانوادهٔ $\{N_i \mid i \in I\}$ است اگر و فقط اگر هر عنصر غیرهمانی G حاصل‌ضرب منحصر به فـردی مانند $a_{i_1}a_{i_2}\cdots a_{i_n}$ باشد که در آن $i_1, \ldots, i_n$ عناصر متمایزی از I اند و به‌ازای هر $k = 1,2,\ldots,n$ ، $e \neq a_{i_k} \in N_{i_k}$* .

برهان. تمرین.

بین حـاصل‌ضربهای‌مستقیم ضعیف داخلی و خارجی تمایز وجود دارد. هرگاه گروه G حاصل‌ضرب مستقیم ضعیـف *داخلی* گروههای N_i باشد، آنگاه، طبق تعریف، هر N_i درواقع زیـرگروهی از G است و G با حاصل‌ضرب مستقیم ضعیف *خارجی* $\prod_{i \in I}^{w} N_i$ یکریخت است. اما حاصل‌ضرب مستقیم ضعیف خارجی $\prod_{i \in I}^{w} N_i$ درواقـع شامل گروههای N_i نیست، بلکه فقط نسخه‌های یکریختی از آنها (یعنی، $(N_i)_i$ ــ ر.ک. قضیهٔ ۴.۸ و تمرین ۱۰) را شامل است. به بیان عملی، این تمایز خیلی مهم نیست و صفات "داخلی" و "خارجی"

وقتی امکان اشتباه نباشد حذف خواهند شد. درواقع، از نماد زیر استفاده می‌کنیم.
نمادگذاری. برای آنکه نشان دهیم گروه G حاصلضرب مستقیم ضعیف داخلی خانوادهٔ زیرگروههایش $\{N_i \mid i \in I\}$ است، می‌نویسیم $G = \prod_{i\in I}^{w} N_i$.

قضیهٔ ۱۰.۸. *فرض کنیم $\{f_i : G_i \to H_i \mid i \in I\}$ خانواده‌ای از همریختیهای گروهها بوده و $f = \prod f_i$ نگاشت $\prod_{i\in I} G_i \to \prod_{i\in I} H_i$ داده شده با $\{a_i\} \mapsto \{f_i(a_i)\}$ باشد. f یک همریختی گروههاست به‌طوری که $f(\prod_{i\in I}^{w} G_i) \subset \prod_{i\in I}^{w} H_i$، $\operatorname{Ker} f = \prod_{i\in I} \operatorname{Ker} f_i$ و $\operatorname{Im} f = \prod_{i\in I} \operatorname{Im} f_i$.*
درنتیجه، f یک تکریختی [یا برووریختی] است اگر و فقط اگر هر f_i چنین باشد.

برهان. تمرین.

نتیجهٔ ۱۱.۸. *فرض کنیم $\{G_i \mid i \in I\}$ و $\{N_i \mid i \in I\}$ خانواده‌هایی از گروهها باشند به طوری که، به‌ازای هر $i \in I$، N_i زیرگروه نرمالی از G_i است.*
(یک) $\prod_{i\in I} N_i$ زیرگروه نرمالی از $\prod_{i\in I} G_i$ بوده و $\prod_{i\in I} G_i/\prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$.
(دو) $\prod_{i\in I}^{w} N_i$ زیرگروه نرمالی از $\prod_{i\in I}^{w} G_i$ بوده و $\prod_{i\in I}^{w} G_i/\prod_{i\in I}^{w} N_i \cong \prod_{i\in I}^{w} G_i/N_i$.

برهان. (یک) به‌ازای هر i، فرض کنیم $\pi_i : G_i \to G_i/N_i$ برووریختی کانونی باشد بنابر قضیهٔ ۱۰.۸، نگاشت $\prod \pi_i : \prod_{i\in I} G_i \to \prod_{i\in I} G_i/N_i$ یک برووریختی با هستهٔ $\prod_{i\in I} N_i$ است. لذا، طبق قضیهٔ اول یکریختی $\prod G_i/\prod N_i \cong \prod G_i/N_i$ اثبات قسمت (دو) به همین ترتیب است.

تمرینات

۱. S_3 حاصلضرب مستقیم خانواده‌ای از زیرگروههای حقیقی خود نیست. همین مطلب در مورد Z_{p^n} (p اول، $n \geq 1$) و $\mathbf{Z}$ صادق است.
۲. گروههای H_i, K_i را طوری مثال بزنید که $H_1 \times H_2 \cong K_1 \times K_2$ و هیچ H_i ی با هیچ K_j یکریخت نباشد.
۳. فرض کنید G یک گروه آبلی (جمعی) با زیرگروههای H و K باشد. نشان دهید

$G \cong H \oplus K$ اگر و فقط اگر همریختیهایی مانند $H \underset{\iota_1}{\overset{\pi_1}{\leftrightarrows}} G \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} K$ وجود داشته باشند به‌طوری‌که $\pi_1\iota_1 = 1_H$ ، $\pi_2\iota_2 = 1_K$ ، $\pi_1\iota_2 = 0$ ، و $\pi_2\iota_1 = 0$ ، که در آن 0 نگاشتی است که هر عنصر را به عنصر صفر (همانی) می‌نگارد، و به‌ازای هر $x \in G$ ، $\iota_1\pi_1(x) + \iota_2\pi_2(x) = x$.

۴ . با مثال نشان دهید که حاصل‌ضرب مستقیم ضعیف یک هم‌حاصل‌ضرب در رستهٔ تمام گروهها نیست . (**راهنمایی .** کافی است دو عامل $G \times H$ را درنظر بگیرید .)

۵ . فرض کنید G, H گروههای دوری متناهی باشند . $G \times H$ دوری است اگر و فقط اگر $(|G|,|H|) = 1$.

۶ . هر گروه‌آبلی با تولید متناهی $G \neq \langle e \rangle$ که هر عنصرش (جز e) از مرتبهٔ p (p اول) باشد با $Z_p \oplus Z_p \oplus \cdots \oplus Z_p$ (n جمعوند) به‌ازای $n \geq 1$ ی یکریخت‌است [**راهنمایی .** فرض کنید $A = \{a_1, \ldots, a_n\}$ مجموعه‌ای از مولدها باشد به‌طوری‌که هیچ زیرمجموعهٔ حقیقی A ، G را تولید نکند . نشان دهید که $\langle a_i \rangle \cong Z_p$ و $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$] .

۷ . فرض کنید H,K,N زیرگروههای نرمال نابدیهی از گروه G بوده و $G = H \times K$. ثابت کنید N در مرکز G است یا N یکی از H,K را به‌طور نابدیهی قطع می‌کند. با مثال نشان دهید که ، وقتی G غیرآبلی باشد ، دو امکان می‌تواند رخ دهد .

۸ . اگر یکی از N_i ها نرمال نباشد ، نتیجهٔ ۷.۸ درست نیست .

۹ . هرگاه گروه G حاصل‌ضرب مستقیم (داخلی) زیرگروههای H,K خود باشد ، آنگاه $H \cong G/K$ و $G/H \cong K$.

۱۰ . هرگاه $\{G_i \mid i \in I\}$ خانواده‌ای از گروهها باشد ، آنگاه $\prod^w G_i$ حاصل‌ضرب مستقیم ضعیف داخلی زیرگروههای $\{\iota_i(G_i) \mid i \in I\}$ می‌باشد .

۱۱ . فرض کنید $\{N_i \mid i \in I\}$ خانواده‌ای از زیرگروههای گروه G باشد . G حاصل‌ضرب مستقیم ضعیف داخلی $\{N_i \mid i \in I\}$ است اگر و فقط‌اگر : (یک) به‌ازای هر $i \neq j$ ، و $a_i \in N_i, a_j \in N_j$ ، $a_ia_j = a_ja_i$ ؛ (دو) هر عنصر غیرهمانی G حاصل‌ضرب منحصر به فردی مانند $a_{i_1} \cdots a_{i_n}$ است ، که در آن $i_1, \ldots, i_n$ عناصر متمایزی از I اند و به ازای هر k ، $e \neq a_{i_k} \in N_{i_k}$. [با قضیهٔ ۹.۸ قیاس کنید .]

۱۲ . زیرگروه نرمال H از گروه G را یک **عامل مستقیم** (**جمعوند مستقیم** اگر G آبلی جمعی باشد) گویند اگر زیرگروه (نرمالی) مانند K از G موجود باشد به‌طوری‌که

$G = H \times K$.

(آ) هرگاه H عامل مستقیمی از K و K عامل مستقیمی از G باشد، آنگاه H در G نرمال است. [با تمرین ۱۰.۵ قیاس کنید.]

(ب) هرگاه H عامل مستقیمی از G باشد، آنگاه هر همریختی $H \to G$ را می‌توان به درونریختیی مانند $G \to G$ توسیع داد. اما یک تکریختی $H \to G$ لزوماً به یک خود ریختی $G \to G$ قابل توسیع نیست.

۱۳. فرض کنید $\{G_i \mid i \in I\}$ خانواده‌ای‌ازگروهها بوده‌و $J \subset I$. نگاشت $\alpha : \coprod_{j\in J} G_j \to \coprod_{i\in I} G_i$ داده شده با $\{a_j\} \mapsto \{b_i\}$، که در آن به‌ازای $j \in J$، $b_i = a_j$ و $i \notin J$، $b_i = e_i$ (G_i یک تکریختی گروههاست و $\coprod_{i\in I} G_i/\alpha(\coprod_{j\in J} G_j) \cong \coprod_{i\in I-J} G_i$ (همانی

۱۴. به‌ازای $i = 1,2$، فرض کنید $H_i \lhd G_i$ و با مثال نشان دهید که هر یک از احکام زیر ممکن است درست نباشد:

(آ) $G_1/H_1 \cong G_2/H_2$ و $G_1 \cong G_2 \Rightarrow G_1/H_1 \cong G_2/H_2$ ؛ $H_1 \cong H_2$

(ب) $G_1/H_1 \cong G_2/H_2$ و $G_1 \cong G_2$ ؛ $\Rightarrow H_1 \cong H_2$

(پ) $G_1/H_1 \cong G_2/H_2$ و $H_1 \cong H_2 \Rightarrow G_1 \cong G_2$.

۹ گروههای آزاد، حاصلضربهای آزاد، و مولدها و رابطه‌ها

نشان خواهیم داد که اشیاء آزاد (گروههای آزاد) در رستهٔ (ملموس) گروهها وجود دارند، و ازاینها روش توصیف گروهها برحسب "مولدها و رابطه‌ها" را به دست می‌آوریم. به علاوه، طرز ساختن هم حاصلضرب (حاصل ضربهای آزاد) در رستهٔ گروهها را نشان خواهیم داد.

با معلوم بودن مجموعهٔ X، گروه F را طوری می‌سازیم که بر X به مفهوم تعریف ۷.۷ آزاد باشد. اگر $X = \varnothing$، F گروه بدیهی $\langle e \rangle$ است. اگر $X \neq \varnothing$، فرض کنیم X^{-1} مجموعه‌ای باشد جدا از X که $|X| = |X^{-1}|$. بیژکسیون $X \to X^{-1}$ را اختیار کرده و نقش $x \in X$ را با x^{-1} نشان می‌دهیم. بالاخره، مجموعه‌ای انتخاب می‌کنیم جدا از $X \cup X^{-1}$ که دقیقاً یک عنصر داشته باشد؛ این عنصر را با 1 نشان می‌دهیم. یک **کلمه** بر X دنباله‌ای است مانند $(a_1,a_2,\ldots)$ با $a_i \in X \cup X^{-1} \cup \{1\}$ به‌طوری‌که به‌ازای $n \in \mathbf{N}^*$ ی و هر $k \geq n$، $a_k = 1$. دنبالهٔ ثابت $(1,1,\ldots)$ **کلمهٔ تهی** نام دارد و با 1 نموده می‌شود. (این نماد مبهم اشکالی ایجاد نخواهد کرد.) کلمهٔ $(a_1,a_2,\ldots)$ بر X را **تحویل**

یافته گویند مشروط بر اینکه

(یک) به‌ازای هر $x \in X$ ، x و x^{-1} مجاورنباشند (یعنی، به‌ازای هر $i \in \mathbf{N}^*$ و $x \in X$ ، $(a_i = x \Rightarrow a_{i+1} \neq x^{-1}$ و $a_i = x^{-1} \Rightarrow a_{i+1} \neq x)$ و

(دو) $a_k = 1$ ایجاب کند که به‌ازای هر $i \geq k$ ، $a_i = 1$.

بخصوص، کلمهٔ تهی 1 تحویل یافته است.

هرکلمهٔ تحویل یافتهٔ ناتهی به شکل $(x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n}1,1,\dots)$ است، که در آن $n \in \mathbf{N}^*$ ، $x_i \in X$ ، و $\lambda_i = \pm 1$ (و، طبق قرارداد، به‌ازای هر $x \in X$ ، x^1 نمایش x می‌باشد). از حالا به بعد، این کلمه را با $x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n}$ نشان خواهیم داد. این نماد جدید راهوارتر و الهام‌بخش‌تر است. توجه کنید که تعریف تساوی دنباله‌ها نشان می‌دهد که دوکلمهٔ تحویل یافتهٔ $x_1^{\lambda_1}\dots x_m^{\lambda_m}$ و $y_1^{\delta_1}\dots y_n^{\delta_n}$ $(x_i,y_j \in X;\ \lambda_i,\delta_j = \pm 1)$ مساویند اگر و فقط اگر هردو 1 باشند یا $m = n$ و به‌ازای هر $i = 1,2,\dots,n$ ، $x_i = y_i, \lambda_i = \delta_i$.

درنتیجه، نگاشت از X به توی مجموعهٔ $F(X)$ مرکب از تمام کلمات تحویل یافته بر X که با $x \to x^1 = x$ داده می‌شود انژکتیو است. X را با نقشش یکی کرده و X را زیرمجموعه‌ای از $F(X)$ در نظر می‌گیریم.

حال بر مجموعهٔ $F = F(X)$ مرکب از تمام کلمات تحویل یافته بر X عملی دوتایی تعریف می‌کنیم. کلمهٔ تهی 1 به عنوان عنصر همانی عمل می‌کند (به‌ازای هر $w \in F$ ، $w1 = 1w = w$). به‌طور غیرصوری، می‌خواهیم، با پهلوی هم گذاشتن، حاصلضرب کلمات تحویل یافتهٔ ناتهی را داشته باشیم؛ یعنی،

$$(x_1^{\lambda_1}\dots x_m^{\lambda_m})(y_1^{\delta_1}\dots y_n^{\delta_n}) = x_1^{\lambda_1}\dots x_m^{\lambda_m}y_1^{\delta_1}\dots y_n^{\delta_n}.$$

متأسفانه، کلمهٔ سمت راست معادله ممکن است تحویل یافته نباشد (مثلا"، اگر $x_m^{\lambda_m} = y_1^{-\delta_1}$). لذا، حاصلضرب را با پهلوی هم گذاشتن و (اگر لازم شد) حذف جملات مجاور به شکل xx^{-1} یا $x^{-1}x$ تعریف می‌کنیم؛ مثلا" ، $(x_1^1x_2^{-1}x_3^1)(x_3^{-1}x_2^1x_4^1) = x_1^1x_4^1$. به‌طور دقیقتر، اگر $x_1^{\lambda_1}\dots x_m^{\lambda_m}$ و $y_1^{\delta_1}\dots y_n^{\delta_n}$ کلمات تحویل‌یافتهٔ ناتهی بر X با خاصیت $m \leq n$ باشند، k را بزرگترین عدد صحیحی می‌گیریم $(0 \leq k \leq m)$ که به‌ازای $j = 0,1,\dots,k-1$ ، $x_{m-j}^{\lambda_{m-j}} = y_{j+1}^{-\delta_{j+1}}$. در این صورت، تعریف می‌کنیم

$$(x_1^{\lambda_1}\dots x_m^{\lambda_m})(y_1^{\delta_1}\dots y_n^{\delta_n}) = \begin{cases} x_1^{\lambda_1}\dots x_{m-k}^{\lambda_{m-k}}y_{k+1}^{\delta_{k+1}}\dots y_n^{\delta_n} & \text{اگر } k < m \\ y_{m+1}^{\delta_{m+1}}\dots y_n^{\delta_n} & \text{اگر } k = m < n \\ 1 & \text{اگر } k = m = n \end{cases}$$

اگر $m > n$ ، حاصلضرب بـه همین نحـو تعریف می‌شود. این تعریف تضمین می‌کند که حاصلضرب کلمات تحویل یافته کلمه‌ای تحویل یافته باشد.

قضیهٔ ۱۰۹. *هرگاه X مجموعه‌ای ناتهی بوده و $F = F(X)$ مجموعهٔ تمام کلمات تحویل یافته بر X باشد، آنگاه F تحت عمل تعریف شده در بالا گروه است و $F = \langle X \rangle$.*

گروه $F = F(X)$ *گروه آزاد بر مجموعهٔ X* نام دارد. (اصطلاح "آزاد" را قضیهٔ ۲۰۹ زیر توضیح داده است.)

طرح برهان ۱۰۹. چون 1 عنصر همانی است و $x_1^{\delta_1}\dots x_n^{\delta_n}$ دارای معکوس $x_n^{-\delta_n}\dots x_1^{-\delta_1}$ است، فقط کافی است شرکتپذیری تحقیق شود. این را می‌توان به استقرا و امتحان خسته کنندهٔ حـالات یـا با طرح ظریفتر زیر انجام داد. به‌ازای هر $x \in X$ و $\delta = \pm 1$ ، فرض کنیم $|x^\delta|$ نگاشت $F \to F$ باشد که با $1 \mapsto x^\delta$ و

$$x_1^{\delta_1}\dots x_n^{\delta_n} \mapsto \begin{cases} \text{اگر } x^\delta \neq x_1^{-\delta_1}\text{ ، } x^\delta x_1^{\delta_1}\dots x_n^{\delta_n} \\ \text{اگر } x^\delta = x_1^{-\delta_1}\text{ ، } x_2^{\delta_2}\dots x_n^{\delta_n} \end{cases}$$

(اگر $n = 1$ ، $= 1$) داده شده است. چون $|x||x^{-1}| = 1_F = |x^{-1}||x|$ ، طبق رابطهٔ (۱۳) درآشنایی، بخش ۳، هر $|x^\delta|$ یک جایگشت (بیژکسیون) از F (با معکوس $|x^{-\delta}|$) است. فرض کنیم $A(F)$ گروه تمام جـایگشتهای F (ر.ک. صفحـهٔ ۳۹) بـوده و F_0 زیرگروه تولید شده به وسیلهٔ $\{|x| \mid x \in X\}$ باشـد. واضـح است کـه نـگاشـت $\varphi : F \to F_0$ داده شـده با $1_F \mapsto 1$ و $x_1^{\delta_1}\dots x_n^{\delta_n} \mapsto |x_1^{\delta_1}|\dots|x_n^{\delta_n}|$ یک سورژکسیون است بـه‌طـوری‌کـه بـه‌ازای هـر $w_i \in F$ ، $\varphi(w_1w_2) = \varphi(w_1)\varphi(w_2)$. چـون تحت نـگاشت $|x_1^{\delta_1}|\dots|x_n^{\delta_n}|$ ، $1 \mapsto x_1^{\delta_1}\dots x_n^{\delta_n}$ ، نتیجه می‌شود که φ انژکتیو است. گروه بودن F_0 ایجاب می‌کند که شرکتپذیری در F برقرار و φ یک یکریختی گروهها باشد. واضح است که $F = \langle X \rangle$.

بعضی از خواص گروههای آزاد به آسانی به دست می‌آیند. مثلاً، هرگاه $|X| \geq 2$ ، آنگاه گروه آزاد بر X غیرآبلی است.

$$(x,y \in X \Rightarrow x^{-1}y^{-1}xy \text{ تحویل یافته است } \Rightarrow x^{-1}y^{-1}xy \neq 1 \Rightarrow xy \neq yx)$$

به همین نحو، هر عنصر در یـک گروه آزاد (جز ۱) مرتبهٔ نامتناهی دارد (تمرین ۱).

هرگاه $X = \{a\}$ ، آنگاه گروه آزاد بر X گروه دوری نامتناهی $\langle a \rangle$ است (تمرین ۲) . نکتهٔ مهم این است که هر زیرگروه از یک گروه آزاد خود یک گروه آزاد بر مجموعه‌ای است (ر.ک. ج . روتمن[1] [۱۹]) .

قضیهٔ ۲۰۹ . فرض کنیم F گروه آزاد بر مجموعهٔ X بوده و $\iota : X \to F$ ، نگاشت شمول باشد . هرگاه G گروه و $f : X \to G$ نگاشتی از مجموعه‌ها باشد، آنگاه همریختی منحصر به فردی از گروهها مانند $\bar{f} : F \to G$ وجود دارد به‌طوری‌که $\bar{f}\iota = f$. به عبارت دیگر، F یک شیء آزاد بر مجموعهٔ X در رستهٔ گروههاست .

تبصره . هرگاه F' شیء آزاد دیگری بر مجموعهٔ X در رستهٔ گروهها (با $\lambda : X \to F'$) باشد، آنگاه قضایای ۸۰۷ و ۲۰۹ ایجاب می‌کنند که یک یکریختی مانند $\varphi : F \cong F'$ وجود داشته باشد که $\varphi\iota = \lambda$. بخصوص، $\lambda(X)$ مجموعهٔ مولدهای F' است؛ این مطلب را می‌توان مستقیماً از تعریف شیء آزاد نیز نتیجه گرفت .

طرح برهان ۲۰۹ . تعریف می‌کنیم $\bar{f}(1) = e$ واگر $x_1^{\delta_1} \cdots x_n^{\delta_n}$ یک کلمهٔ تحویل یافتهٔ ناتهی بر X باشد، تعریف می‌کنیم $\bar{f}(x_1^{\delta_1} \cdots x_n^{\delta_n}) = f(x_1)^{\delta_1} f(x_2)^{\delta_2} \cdots f(x_n)^{\delta_n}$. چون G گروه است و $\delta_i = \pm 1$ ، حاصل ضرب $f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n}$ عنصر تعریف شده‌ای از G است . تحقیق کنید که $\bar{f}$ یک همریختی است به‌طوری‌که $\bar{f}\iota = f$. هرگاه $g : F \to G$ یک همریختی باشد به‌طوری‌که $g\iota = f$ ، آنگاه

$$g(x_1^{\delta_1} \cdots x_n^{\delta_n}) = g(x_1^{\delta_1}) \cdots g(x_n^{\delta_n}) = g(x_1)^{\delta_1} \cdots g(x_n)^{\delta_n} = g\iota(x_1)^{\delta_1} \cdots g\iota(x_n)^{\delta_n}$$
$$= f(x_1)^{\delta_1} \cdots f(x_n)^{\delta_n} = \bar{f}(x_1^{\delta_1} \cdots x_n^{\delta_n}).$$

لذا، $\bar{f}$ منحصر به فرد است .

نتیجهٔ ۲۰۹ . هر گروه G نقش همریخت یک گروه آزاد است .

برهان . فرض کنیم X مجموعه‌ای از مولدهای G بوده و F گروه آزاد برمجموعهٔ X باشد .

---

1. J. Rotman

طبق قضیهٔ ۲۰۹ ، نگاشت شمول $X \to G$ همریختی $\bar{f}: F \to G$ را القا می‌کند به‌طوری که $x \mapsto x \in G$. چون $G = \langle X \rangle$ ، برهان‌قضیهٔ ۲۰۹ نشان می‌دهدکه $\bar{f}$ یک برووریختی است .

از نتیجهٔ ۳۰۹و قضیهٔ اول یکریختی فورا" معلوم می‌شود که هر گروه G با یک گروه خارج قسمتی مانند F/N یکریخت است ، که در آن $G = \langle X \rangle$ ، F گروه آزاد بر X ، و N هستهٔ برووریختی $F \to G$ درنتیجهٔ ۳۰۹ است . لذا ، برای توصیف G با تقریب یکریختی ، کافی است X ، F ، و N را مشخص کنیم . اما F به‌وسیلهٔ X با تقریب یکریختی معین می‌شود (قضیهٔ ۸۰۷) و N با هر زیرمجموعه که آن را به‌صورت زیرگروهی از F تولید کند مشخص می‌گردد . اما ، هرگاه $w = x_1^{\delta_1} \cdots x_n^{\delta_n} \in F$ یک‌مولد N باشد ، آنگاه تحت برووریختی $F \to G$ ، $w \mapsto x_1^{\delta_1} \cdots x_n^{\delta_n} = e \in G$. معادلهٔ $x_1^{\delta_1} \cdots x_n^{\delta_n} = e$ در G یک *رابطه* بر مولدهای x_i نامیده می‌شود . واضح است که گروه G را می‌توان با مشخص کردن مجموعهٔ X از مولدهای G و مجموعهٔ مناسب R از رابطه‌ها بر این مولدها کاملا" توصیف کرد . این توصیف منحصر به فرد نیست ، زیرا ، به‌ازای گروه داده شدهٔ G ، X و R را می‌توان به طرق بسیار انتخاب کرد (ر.ک. تمرینات ۶ و ۹) .

به‌عکس، فرض کنیم مجموعهٔ X و مجموعهٔ Y از کلمات (تحویل یافته) بر عناصر X داده شده باشند . سوءال : آیا گروهی مانند G هست که G به وسیلهٔ X تولید شده و تمام روابط $(w \in Y)\, w = e$ برقرار باشند (که در اینجا $w = x_1^{\delta_1} \cdots x_n^{\delta_n}$ حاصلضرب در G را نشان می‌دهد) ؟ خواهیم دید که جواب مثبت است ، مشروط بر اینکه در گروه G عناصر X لزوما" همه متمایز نباشند . به عنوان مثال ، هرگاه $a,b \in X$ و a^1b^{-1} یک کلمهٔ (تحویل‌یافته) در Y باشد ، آنگاه درهر گروه شامل a,b و صادق در $a^1b^{-1} = e$ باید داشته باشیم $a = b$.

مجموعهٔ X از "مولدها" و مجموعهٔ Y ازکلمات (تحویل یافته) بر عناصر X داده شده‌اند . یک چنین گروه را به صورت زیر می‌سازیم . فرض کنیم F گروه آزاد بر X بوده و N زیرگروه *نرمال* F تولید شده به وسیلهٔ Y باشد[1] ! فرض کنیم G گروه خارج قسمتی F/N بوده و X بانقشش در F/N تحت نگاشت $X \subset F \to F/N$ یکی شده باشد .

---

۱. *زیرگروه نرمال تولید شده به وسیلهٔ مجموعهٔ $S \subset F$ اشتراک تمام زیرگروههای نرمال F است که شامل S می‌باشند ؛ ر.ک. تمرین ۲۰۵ .*

همانطور که در بالاگفتیم ،این ممکن است مستلزم یکی کردن بعضی از عناصر X با یکدیگر باشد. دراین‌صورت ، G گروه تولید شده به وسیلهٔ X (تحت انطباقها) بوده و، بنابر نحوهٔ ساختن ، تمام روابط $(w \in Y)\ w = e$ برقرارند

$$(w = x_1^{\delta_1} \cdots x_n^{\delta_n} \in Y \Rightarrow x_1^{\delta_1} \cdots x_n^{\delta_n} \in N \Rightarrow x_1^{\delta_1} N \cdots x_1^{\delta_n} N = N$$

یعنی ، در $G = F/N$ ، $(x_1^{\delta_1} \cdots x_n^{\delta_n} = e$

تعریف ۴۰۹ . فرض‌کنیم X یک مجموعه و Y مجموعهٔ کلمات (تحویل‌یافته) بر X باشد. گروه G را گروه تعریف شده به وسیلهٔ مولدهای $x \in X$ و روابط $(w \in Y)\ w = e$ گویند اگر $G \cong F/N$ ، که در آن F گروه آزاد بر X بوده و N زیرگروه نرمال F تولید شده به وسیلهٔ Y است. می‌گویند $(X \mid Y)$ یک نمایش G است.

بحث قبلی نشان می‌دهد که گروه تعریف شده به وسیلهٔ مولدها و روابط داده شده همیشه وجود دارد. به‌علاوه ، این بزرگترین گروه از این نوع به معنی زیر است.

قضیهٔ ۵۰۹ . (وان دایک[1]) . *فرض کنیم X یک مجموعه ، Y مجموعه‌ای از کلمات (تحویل یافته) بر X ، و G گروه تعریف شده به وسیلهٔ مولدهای $x \in X$ و روابط $(w \in Y)\ w = e$ باشد. هرگاه H یک گروه باشد به‌طوری‌که $H = \langle X \rangle$ و H در تمام روابط $(w \in Y)\ w = e$ صدق کند ، آنگاه یک برووریختی مانند $G \to H$ وجود دارد.*

تبصره. عناصر Y به عنوان کلمات بر X تعبیر شده‌اند ، حاصلضربها در G اند ، و در جایی که از قراین برآید ، حاصلضربها در H می‌باشند.

برهان ۵۰۹ . هرگاه F گروه‌آزاد بر X باشد ، آنگاه ، طبق نتیجهٔ ۳۰۹ ، نگاشت شمول $X \to H$ یک برووریختی مانند $\varphi : F \to H$ القا می‌کند. چون H در روابط $(w \in Y) w = e$ صدق می‌کند ، $Y \subset \operatorname{Ker} \varphi$. درنتیجه ، زیرگروه نرمال N تولید شده به وسیلهٔ Y در F مشمول $\operatorname{Ker} \varphi$ است. طبق نتیجهٔ ۸۰۵ ، φ یک برووریختی $F/N \to H/0$ القا خواهد

---

1. *Van Dyck*

کرد. بنابراین، ترکیب $G \cong F/N \to H/0 \cong H$ یک بروریختی می‌باشد.

گروههای زیر که به وسیلهٔ مولدها و روابط تعریف شده‌اند نوع خاصی از استدلالها را نشان می‌دهند که اغلب تنها راه بررسی یک نمایش است. هرجا مناسب بود، از نماد نمایی برای کلمات استفاده خواهیم کرد (مثلاً "x^2y^{-3}" به جای $xxyyy^{-1}y^{-1}y^{-1}$).

مثال. فرض‌کنیم G گروه تعریف‌شده به‌وسیلهٔ مولدهای a,b و روابط $a^4 = e$، $a^2b^{-2} = e$، و $abab^{-1} = e$ باشد. چون Q_8، یعنی گروه چهارتایی از مرتبهٔ 8، تولید شده به وسیلهٔ عناصر a,b، در این روابط صدق می‌کند (تمرین ۱۴.۴)، بنابر قضیهٔ ۵.۹، یک بروریختی مانند $\varphi : G \to Q_8$ وجود دارد. لذا، $|G| \geq |Q_8| = 8$. فرض‌کنیم F گروه آزاد بر $\{a,b\}$ بوده و N زیرگروه نرمال تولید شده به وسیلهٔ $\{a^4, a^2b^{-2}, abab^{-1}\}$ باشد. به آسانی معلوم می‌شود که هر عنصر F/N به شکل a^ib^jN است با $0 \leq i \leq 3$ و $j = 0,1$، که از آنجا $|F/N| \leq 8 = |G|$. بنابراین، $|G| = 8$ و φ یک یکریختی است. لذا، گروه تعریف شده با مولدها و روابط داده شده با Q_8 یکی (یکریخت) است.

مثال. گروه تعریف شده با مولدهای a,b و روابط $a^n = e$ $(3 \leq n \in \mathbf{N}^*)$، $b^2 = e$، و $abab = e$ (یا $ba = a^{-1}b$) گروه دو وجهی D_n است (تمرین ۸).

مثال. گروه تعریف شده با یک مولد b و یک رابطه مانند $b^m = e$ $(m \in \mathbf{N}^*)$ مساوی Z_m است (تمرین ۹).

مثال. گروه آزاد F بر مجموعهٔ X گروه تعریف شده با مولدهای $x \in X$ وهیچ رابطه‌است (به یاد آورید که، طبق تعریف ۷.۲، $\langle \varnothing \rangle = \langle e \rangle$). اصطلاح "آزاد" از این امر که F از رابطه آزاد است ناشی شده است.

این بخش را با بحث کوتاهی از هم‌حاصل‌ضربها (حاصل‌ضربهای آزاد) در رستهٔ گروهها به پایان می‌بریم. اغلب توضیحات به خواننده محول شده است، زیرا روند شبیه ساختن گروههای آزاد است.

خانوادهٔ $\{G_i \mid i \in I\}$ از گروهها داده شده است. می‌توان فرض کرد (با تجدید

برچسب در صورت لزوم) که G_i ها مجموعه‌هایی دو به دو از هم جدا باشند . فرض کنیم $X = \bigcup_{i\in I} G_i$ و $\{1\}$ مجموعه‌ای تک عنصری جدا از X باشد . یک **کلمه** بر X دنباله‌ای است مانند $(a_1,a_2,\ldots)$ به‌طوری‌که $a_i \in X \cup \{1\}$ وبه‌ازای $n \in \mathbf{N}^*$ ی ،به‌ازای‌هر $i \geq n$ ، $a_i = 1$.
کلمهٔ $(a_1,a_2,\ldots)$ **تحویل یافته** است اگر
(یک) هیچ $a_i \in X$ ی عنصر همانی در گروه خود G_i نباشد ؛
(دو) به‌ازای هر $i,j \geq 1$ ، a_i و a_{i+1} در یک گروه G_j **نباشند** ؛
(سه) $a_k = 1$ ایجاب کند که به‌ازای هر $i \geq k$ ، $a_i = 1$.
بخصوص، $(1,1,\ldots) = 1$ تحویل یافته است . هر کلمهٔ تحویل یافتهٔ $(\neq 1)$ را می‌توان به طور منحصر به‌فرد به‌صورت $a_1a_2\cdots a_n = (a_1,a_2,\ldots,a_n,1,1,\ldots)$ نوشت ،که در آن $a_i \in X$.
فرض کنیم $\prod^*_{i\in I} G_i$ (یا $G_1 * G_2 * \cdots * G_n$ اگر I متناهی باشد) مجموعهٔ تمام کلمات تحویل‌یافته بر X باشد . $\prod^*_{i\in I} G_i$ گروهی تشکیل می‌دهد ، به‌نام **حاصل‌ضرب آزاد** خانوادهٔ $\{G_i \mid i \in I\}$ ، تحت‌عملی‌دوتایی که به صورت زیر تعریف شده است . 1 عنصر همانی است و حاصل‌ضرب دو کلمهٔ تحویل یافته $(\neq 1)$ اساسا " با پهلوی هم گذاشتن تعریف می‌شود . چون حاصل ضرب پهلوی هم گذاشته شدهٔ دو کلمهٔ تحویل یافته ممکن است تحویل یافته نباشد ، باید حذف و ادغامهای لازم را در آن انجام داد . مثلا " ، هرگاه به‌ازای $i = 1,2,3$ ، $a_i,b_i \in G_i$ ، آنگاه

$$(a_1a_2a_3)(a_3^{-1}b_2b_1b_3) = a_1c_2b_1b_3 = (a_1,c_2,b_1,b_3,1,1,\ldots),$$

که در آن $c_2 = a_2b_2 \in G_2$. بالاخره ، به‌ازای هر $k \in I$ ، نگاشت $\iota_k : G_k \to \prod^*_{i\in I} G_i$ داده شده با $e \mapsto 1$ و $a \mapsto a = (a,1,1,\ldots)$ یک تکریختی گروههاست . درنتیجه ، ما گاهی G_k را با نقش یکریخت آن در $\prod^*_{i\in I} G_i$ یکی می‌کنیم (مثلا " ، تمرین ۱۵) .

قضیهٔ ۶.۹ . فرض کنیم $\{G_i \mid i \in I\}$ **خانواده‌ای از گروهها بوده و** $\prod^*_{i\in I} G_i$ **حاصل‌ضرب آزاد آنها باشد . هرگاه** $\{\psi_i : G_i \to H \mid i \in I\}$ **خانواده‌ای از همریختیهای گروهها باشد ،آنگاه همریختی منحصر به فردی مانند** $\psi : \prod^*_{i\in I} G_i \to H$ **وجود دارد به‌طوری‌که به‌ازای هر** $i \in I$ ، $\psi\iota_i = \psi_i$ ، **واین‌خاصیت** $\prod^*_{i\in I} G_i$ **را به‌طور منحصربه فرد با تقریب یکریختی معین می‌کند .**

به‌عبارت دیگر، $\coprod_{i\in I}^{*} G_i$ یک هم‌حاصل‌ضرب در رستهٔ گروههاست.

طرح برهان. اگر $a_1a_2\cdots a_n$ یک کلمهٔ تحویل یافته در $\coprod_{i\in I}^{*} G_i$ با $a_k \in G_{i_k}$ باشد، $\psi(a_1\cdots a_n)$ را مساوی $\psi_{i_1}(a_1)\psi_{i_2}(a_2)\cdots\psi_{i_n}(a_n) \in H$ تعریف کنید.

تمرینات

۱. هر عنصر غیرهمانی در گروه آزاد F دارای مرتبهٔ نامتناهی است.

۲. نشان دهید که گروه آزاد بر مجموعهٔ $\{a\}$ یک گروه دوری نامتناهی است؛ و در نتیجه، با $\mathbf{Z}$ یکریخت است.

۳. فرض کنید F گروهی آزاد بوده و N زیرگروه تولید شده به وسیلهٔ مجموعهٔ $\{x^n \mid x \in F\}$، n عدد صحیح ثابتی است $(|)$ باشد. نشان دهید که $N \lhd F$.

۴. فرض کنید F گروه آزاد بر مجموعهٔ X بوده، و $Y \subset X$. هرگاه H کوچکترین زیرگروه نرمال F شامل Y باشد، آنگاه F/H یک گروه آزاد است.

۵. گروه تعریف شده با مولدهای a,b و روابط $a^8 = b^2a^4 = ab^{-1}ab = e$ مرتبه‌ای حداکثر 16 دارد.

۶. گروه دوری مرتبهٔ 6 گروه تعریف شده به وسیلهٔ مولدهای a,b و روابط $a^2 = b^3 = a^{-1}b^{-1}ab = e$ است.

۷. نشان دهید که گروه تعریف شده به وسیلهٔ مولدهای a,b و روابط $a^2 = e, b^3 = e$ نامتناهی و غیرآبلی است.

۸. گروه تعریف شده به وسیلهٔ مولدهای a,b و روابط $a^n = e \ (3 \le n \in N^*)$، $b^2 = e$، و $abab = e$ گروه دو وجهی D_n است. [ر.ک. قضیهٔ ۱۳۰۶.]

۹. گروه تعریف شده به وسیلهٔ مولد b و رابطهٔ $b^m = e \ (m \in N^*)$ گروه دوری Z_m است.

۱۰. عمل ضرب آزاد تعویضپذیر و شرکتپذیر است: به‌ازای هر سه گروه A,B,C، $A * B \cong B * A$ و $A * (B * C) \cong (A * B) * C$.

۱۱. هرگاه N زیرگروه نرمال $A * B$ تولیدشده به‌وسیلهٔ A باشد، آنگاه $(A * B)/N \cong B$.

۱۲. هرگاه G و H هر یک بیش از یک عنصر داشته باشد، آنگاه $G * H$ یک گروه نامتناهی با مرکز (e) است.

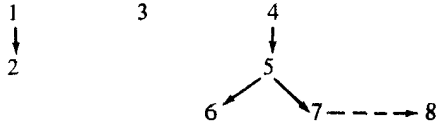
۱۳. هر گروه آزاد یک حاصل‌ضرب آزاد از گروههای دوری نامتناهی است.

۱۴ . هرگاه G گروه تعریف شده به وسیلهٔ مولدهای a,b و روابط $a^2 = e, b^3 = e$ باشد ، آنگاه $G \cong Z_2 * Z_3$. [ر.ک. تمرین ۱۲ و قیاس کنید با تمرین ۶ .]

۱۵ . هرگاه $f : G_1 \to G_2$ و $g : H_1 \to H_2$ همریختیهایی از گروهها باشند ، آنگاه همریختی منحصر به فردی مانند $h : G_1 * H_1 \to G_2 * H_2$ هست به‌طوری‌که $h \mid G_1 = f$ و $h \mid H_1 = g$.

۲ ساختار گروهها

مطالعهٔ خود از گروهها را طبق طرحی که در مقدمهٔ فصل ۱ بیان شد ادامه می‌دهیم. تاکید اصلی اثبات قضایای ساختاریی نسبتا "عمیق در باب رده‌هایی از گروههای آبلی و رده‌های مختلفی از گروهها (احتمالا "غیرآبلی) است که در خواص مطلوبی با گروههای آبلی سهیم‌اند. فصل حاضر دارای سه قسمت اصلی است که اساسا "از هم مستقل‌اند، جز آنکه نتایج یکی ممکن است به عنوان مثال یا انگیزه در دیگری به کار رود. ارتباط بین بخشها به‌صورت زیر است:



اکثر مطالب بخش ۸ از بقیهٔ فصل مستقل است.

۱ گروههای آبلی آزاد

اشیاء آزاد در رستهٔ گروههای آبلی را مورد بررسی قرار می‌دهیم. همانطورکه در رابطه با گروههای آبلی مرسوم است، *در سراسر این بخش از نماد جمعی استفاده می‌شود*. فرهنگ لغت زیر ممکن است مفید واقع شود.

ab ..... $a + b$
a^{-1} ..... $-a$
e 0
a^n ..... na

ab^{-1}	$a - b$
HK	$H + K$
aH	$a + H$
$G \times H$	$G \oplus H$
$H \vee K$	$H + K$
$\prod_{i \in I}^{w} G_i$	$\sum_{i \in I} G_i$
مجموع مستقیم	حاصلضرب مستقیم ضعیف

در هر گروه G با نماد جمعی، $(a \in G;\ m,n \in \mathbf{Z})\ (m+n)a = ma + na$. هرگاه گروه آبلی باشد، آنگاه $m(a+b) = ma + mb$. هرگاه X زیرمجموعه‌ای ناتهی از G باشد، آنگاه طبق قضیهٔ I . ۸.۲ ، زیرگروه $\langle X \rangle$ تولید شده به وسیلهٔ X در نماد جمعی مرکب از جمیع *ترکیبات خطی* $n_1x_1 + n_2x_2 + \cdots + n_kx_k$ $(n_i \in \mathbf{Z},\ x_i \in X)$ است . بخصوص، گروه دوری $\langle x \rangle$ عبارت است از $\{nx \mid n \in \mathbf{Z}\}$.

یک **پایهٔ** گروه آبلی F زیرمجموعه‌ای است مانند X از F به‌طوری‌که (یک) $\langle X \rangle = F$ ؛ و (دو) برای عناصر متمایز $x_1, x_2, \ldots, x_k \in X$ و $n_i \in \mathbf{Z}$ ،

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0 \quad \Rightarrow \quad n_i = 0,\ i$$

به‌ازای هر خواننده نباید به خاطر شباهت با پایه‌های فضاهای برداری گمراه شود . (تمرین ۲) .

قضیهٔ ۱۰۱ . *شرایط زیر در مورد گروه آبلی* F *معادلند* :

(یک) F *یک پایهٔ ناتهی دارد* ؛

(دو) F *مجموع مستقیم (داخلی) خانواده‌ای نامتناهی از زیرگروههای دوری است* ؛

(سه) F *مساوی (یکریخت) با مجموع مستقیم نسخه‌هایی از گروه جمعی* $\mathbf{Z}$ *از اعداد صحیح است* .

(چهار) *مجموعه‌ای ناتهی مانند* X *و تابعی چون* $f : X \to F$ ، *با خاصیت زیر وجود دارند* : *به‌ازای گروه آبلی* G *و تابع* $f : X \to G$ ، *همریختی منحصر به فردی از گروهها مانند* $\bar{f} : F \to G$ *وجود دارد به‌طوری‌که* $\bar{f}i = f$. *به عبارت دیگر*، F *یک‌شیٔ آزاد در رستهٔ گروههای آبلی است*.

گروه آبلی F صادق در شرایط قضیهٔ ۱۰۱ یک **گروه آبلی آزاد** (بر مجموعهٔ X) نامیده می‌شود . طبق تعریف، گروه بدیهی 0 گروه آبلی آزاد بر مجموعهٔ پوچ $\varnothing$ است .

طرح برهان ۱۰۱ . (دو) $\Rightarrow$ (یک) هرگاه X پایه‌ای از F باشد، آنگاه به‌ازای هر $x \in X$، $nx = 0$ اگروفقطاگر $n = 0$، ازاینرو، هر زیر گروه $\langle x \rangle$ $(x \in X)$ یک گروه دوری نامتناهی (ونرمال زیرا F آبلی است) است. چون $F = \langle X \rangle$، نیز داریم $F = \bigcup_{x \in X} \langle x \rangle$.

هرگاه به‌ازای $z \in X$ ی، $\langle z \rangle \cap \bigcup_{\substack{x \in X \\ x \neq z}} \langle x \rangle \neq 0$، آنگاه به‌ازای $n \in \mathbf{Z}$ ناصفری، $nz = n_1x_1 + \cdots + n_kx_k$، که در آن $z, x_1, \ldots, x_k$ عناصر متمایزی از X اند، که با پایه بودن X متناقض است. لذا، $\langle z \rangle \cap \bigcup_{\substack{x \in X \\ x \neq z}} \langle x \rangle = 0$؛ ودرنتیجه، طبق تعریف I ۸۰۸۰، $F = \sum_{x \in X} \langle x \rangle$.

(سه) $\Rightarrow$ (دو) قضایای I ۳۰۳۰ ۲، I ۶۰۸۰، و I ۱۰۸۰.

(یک) $\Rightarrow$ (سه) فرض کنیم $F \cong \sum \mathbf{Z}$ و نسخه‌های $\mathbf{Z}$ با مجموعهٔ X اندیسگذاری شده باشند. به‌ازای هر $x \in X$، θ_x عنصر $\{u_i\}$ از $\sum \mathbf{Z}$ باشد که به‌ازای $i \neq x$، $u_i = 0$، و $u_x = 1$. تحقیق کنید که $\{\theta_x \mid x \in X\}$ پایه‌ای از $\sum \mathbf{Z}$ است و، با استفاده از یکریختی $F \cong \sum \mathbf{Z}$، پایه‌ای برای F به دست آورید.

(چهار) $\Rightarrow$ (یک) فرض کنیم X پایه‌ای از F بوده و $\iota : X \to F$ نگاشت شمول باشد. همچنین، نگاشت $f : X \to G$ داده‌شده باشد. هرگاه $u \in F$، آنگاه $u = n_1x_1 + \cdots + n_kx_k$ $(n_i \in \mathbf{Z}; x_i \in X)$، زیرا X، F راتولید می‌کند. هرگاه $(m_k \in \mathbf{Z})u = m_1x_1 + \cdots + m_kx_k$، آنگاه $\sum_{i=1}^{k} (n_i - m_i)x_i = 0$، که از آنجا به‌ازای هر i، $n_i = m_i$، زیرا X یک پایه است. درنتیجه، نگاشت $\bar{f} : F \to G$ داده‌شده‌با $\bar{f}(u) = \bar{f}\left(\sum_{i=1}^{k} n_ix_i\right) = n_1f(x_1) + \cdots + n_kf(x_k)$ تابع تعریف شده‌ای است که $\bar{f}\iota = f$. چون G آبلی است، به آسانی دیده می‌شود که $\bar{f}$ همریختی‌است. چون X، F را تولید می‌کند، هر همریختی $F \to G$ کاملا" با عملش بر X معین می‌شود. لذا، هرگاه $g : F \to G$ یک همریختی باشد به‌طوری‌که $g\iota = f$، آنگاه به‌ازای هر $x \in X$، $g(x) = g(\iota(x)) = f(x) = \bar{f}(x)$؛ درنتیجه، $g = \bar{f}$ و $\bar{f}$ منحصر به فرد است. بنابراین، طبق تعریف I ۷۰۷۰، F یک شئ آزاد بر مجموعهٔ X در رستهٔ گروههای آبلی است.

(سه) $\Rightarrow$ (چهار). به فرض آنکه $\iota : X \to F$، مجموع مستقیم $\sum \mathbf{Z}$ با نسخه‌هایی از $\mathbf{Z}$ که با X اندیسگذاری شده است را می‌سازیم. فرض کنیم $Y = \{\theta_x \mid x \in X\}$ مثل برهان

(یک) ⇒ (سه) پایه‌ای از $\sum \mathbf{Z}$ باشد. برهان (چهار) ⇒ (یک) ⇒ (سه) نشان می‌دهد که $\sum \mathbf{Z}$ یک شیء آزاد بر مجموعهٔ Y است. چون بوضوح داریم $|Y| = |X|$، طبق قضیهٔ I ، ۸.۷ ، ۱ $F \cong \sum \mathbf{Z}$.

به فرض معلوم بودن X، برهان قضیهٔ ۱۰۱ طرز ساختن گروه آبلی آزاد F با پایهٔ X را نشان می‌دهد. کافی است F را مجموع مستقیم $\sum \mathbf{Z}$ بگیریم با نسخه‌هایی از $\mathbf{Z}$ که به وسیلهٔ X اندیسگذاری شده‌اند. مثل برهان (یک) ⇒ (سه)، $\{\theta_x \mid x \in X\}$ یک پایهٔ $F = \sum \mathbf{Z}$ بوده، و F بر مجموعهٔ $\{\theta_x \mid x \in X\}$ آزاد است. چون نگاشت $\iota : X \to F$ داده شده با $x \mapsto \theta_x$ انژکتیو است، به آسانی معلوم می‌شود که F بر X به معنی شرط (چهار) قضیهٔ ۱۰۱ آزاد است. در این وضع، X را با نقشش تحت ι یکی می‌کنیم؛ درنتیجه، $X \subset F$ و زیرگروه دوری $\mathbf{Z}\theta_x = \{n\theta_x \mid n \in \mathbf{Z}\}$ به‌صورت $\langle \theta_x \rangle = \mathbf{Z}x$ نوشته می‌شود. با این نماد، $F = \sum_{x \in X} \langle \theta_x \rangle$ به صورت $F = \sum_{x \in X} \mathbf{Z}x$ نوشته می‌شود، و عنصر نوعی F به شکل $(n_i \in \mathbf{Z}, x_i \in X)\ n_1x_1 + \cdots + n_kx_k$ می‌باشد. بخصوص، $X = \iota(X)$ یک پایهٔ F می‌باشد.

قضیهٔ ۲۰۱. هر دو پایه از گروه آبلی آزاد F یک اصلیت دارند.

لذا، عدد اصلی پایهٔ X از گروه آبلی آزاد F یک پایای F است؛ $|X|$ **رتبهٔ** F نام دارد.

طرح برهان ۲۰۱. ابتدا فرض کنید F دارای پایه‌ای مانند X با اصلیت متناهی n باشد؛ درنتیجه، (n جمعوند) $F \cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$. به‌ازای هر زیرگروه G از F، تحقیق کنید که $2G = \{2u \mid u \in G\}$ زیرگروهی از G است. و نیز تحقیق کنید که تحدید یکریختی $F \cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$ به $2F$ یکریختی $2\mathbf{Z} \oplus \cdots \oplus 2\mathbf{Z} \cong 2F$ است، که از آنجا، طبق نتیجهٔ I ، ۱۱.۸ ، ۱

$$F/2F \cong \mathbf{Z}/2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/2\mathbf{Z} \cong Z_2 \oplus \cdots \oplus Z_2 \quad (n \text{ جمعوند})$$

بنابراین، $|F/2F| = 2^n$. هرگاه Y پایهٔ دیگری از F بوده و r عدد صحیحی باشد به طوری‌که $|Y| \geq r$، آنگاه استدلالی مشابه نشان می‌دهد که $|F/2F| \geq 2^r$، که از آنجا

$2^r \leq 2^n$ و $r \leq n$. پس نتیجه می‌شود که $|Y| = m \leq n$ و $|F/2F| = 2^m$. بنابراین ، $|X| = n = m = |Y|$ و $2^m = 2^n$.

هرگاه یکی از پایه‌های F نامتناهی باشد ، آنگاه ، بنابر بند پیش ، تمام پایه‌ها نامتناهی‌اند . درنتیجه ، برای اتمام برهان کافی است نشان دهیم که اگر X یک پایهٔ نامتناهی **دلخواه** F باشد، $|F| = |X|$. واضح است که $|F| \leq |X|$. فرض کنیم $S = \bigcup_{n \in \mathbf{N}^*} X^n$ ، که در آن (n عامل) $X^n = X \times \cdots \times X$. به‌ازای هر $s = (x_1, \ldots, x_n) \in S$ ، فرض کنیم G_s زیرگروه $\langle x_1, \ldots, x_n \rangle$ باشد . در این‌صورت ، $G_s \cong \mathbf{Z}y_1 \oplus \cdots \oplus \mathbf{Z}y_t$ ، که در آن $y_1, \ldots, y_t$ $(t \leq n)$ عنصرهای متمایز $\{x_1, \ldots, x_n\}$ اند . لذا ، طبق آشنایی ، قضیهٔ ۱۲۰۸ ، $|G_s| = |\mathbf{Z}^t| = |\mathbf{Z}| = \aleph_0$. چون $F = \bigcup_{s \in S} G_s$ ، بنابر آشنایی ، تمرین ۱۲۰۸ ، $|F| = |\bigcup_{s \in S} G_s| \leq |S|\aleph_0$. بنابر آشنایی ، قضیهٔ ۱۱۰۸ و ۱۲۰۸ ، $|S| = |X|$ ، که از آنجا $|F| \leq |X|\aleph_0 = |X|$. بنابراین ، طبق قضیهٔ شرودر ــ برنشتاین ، $|F| = |X|$.

حکم ۳۰۱ . *فرض کنیم F_1 گروه آبلی آزاد بر مجموعهٔ X_1 ، و F_2 گروه آبلی آزاد بر مجموعهٔ X_2 باشد . در این‌صورت ، $F_1 \cong F_2$ اگر و فقط اگر F_1 و F_2 یک رتبه داشته باشند (یعنی ، $|X_1| = |X_2|$) .*

تبصره . حکم ۳۰۱ برای گروههای آزاد غیرآبلی دلخواه (مثل بخش I . ۹) نیز برقرار است ؛ ر.ک. تمرین ۱۲ .

طرح برهان ۳۰۱ . هرگاه $\alpha : F_1 \cong F_2$ ، آنگاه $\alpha(X_1)$ پایه‌ای از F_2 است ، که از آنجا ، بنابر قضیهٔ ۲۰۱ ، $|X_1| = |\alpha(X_1)| = |X_2|$. عکس مطلب قضیهٔ I . ۸۰۷ است .

قضیهٔ ۴۰۱ . *هر گروه آبلی G نقش‌همریخت یک گروه آبلی آزاد از رتبهٔ $|X|$ است ، که X مجموعه‌ای از مولدهای G می‌باشد .*

برهان . فرض کنیم F گروه آبلی آزاد بر مجموعهٔ X باشد . در این صورت ، $F = \sum_{x \in X} \mathbf{Z}x$ ،

و $|X| =$ رتبهٔ F . بنابر قضیهٔ ۱۰۱ ، نگاشت شمول $X \to G$ یک همریختی مانند $\bar{f} : F \to G$ القا می‌کند به‌طوری‌که $1x \mapsto x \in G$ ، که از آنجا $X \subset \operatorname{Im} \bar{f}$. چون X ، G را تولید می‌کند ، باید داشته باشیم $\operatorname{Im} \bar{f} = G$.

حال قضیه‌ای ثابت می‌کنیم که در تحلیل ساختار گروههای آبلی با تولید متناهی بسیار مهم است (بخش ۲) . به لم زیر نیاز خواهیم داشت .

لم ۵۰۱ . *هرگاه $\{x_1, \ldots, x_n\}$ پایه‌ای از گروه آبلی آزاد F بوده و $a \in \mathbf{Z}$ ، آنگاه به‌ازای هر $i \neq j$ ، $\{x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\}$ نیز پایه‌ای از F می‌باشد .*

برهان . چون $x_j = -ax_i + (x_j + ax_i)$ ، نتیجه می‌شود که

$$F = \langle x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n \rangle .$$

هرگاه $(k_i \in \mathbf{Z}) k_1x_1 + \cdots + k_j(x_j + ax_i) + \cdots + k_nx_n = 0$ ، آنگاه

$$k_1x_1 + \cdots + (k_i + k_ja)x_i + \cdots + k_jx_j + \cdots + k_nx_n = 0,$$

ایجابگر آنکه به‌ازای هر t ، $k_t = 0$.

قضیهٔ ۶۰۱ . *هرگاه F یک گروه آبلی آزاد از رتبهٔ متناهی n بوده و G زیرگروه ناصفری از F باشد ، آنگاه پایه‌ای مانند $\{x_1, \ldots, x_n\}$ از F ، عدد صحیحی مانند r $(1 \leq r \leq n)$ ، و اعداد صحیح مثبتی مانند $d_1, \ldots, d_r$ وجود دارند به‌طوری‌که $d_1 \mid d_2 \mid \cdots \mid d_r$ و G گروه آبلی با پایهٔ $\{d_1x_1, \ldots, d_rx_r\}$ است .*

چند تبصره . هر زیر گروه یک گروه آبلی آزاد (احتمالاً نامتناهی) از رتبهٔ α آزاد و از رتبهٔ حداکثر α است ؛ ر.ک. قضیهٔ IV ۱۰۶ . نماد "$d_1 \mid d_2 \mid \ldots \mid d_r$" یعنی "$d_1$ عاد می‌کند d_2 ، d_2 عاد می‌کند d_3 ، و غیره ."

برهان ۶۰۱ . هرگاه $n = 1$ ، آنگاه ، طبق قضایای I ۵۰۳۰ ، I ۱۰۳۰ ، و I ۲۰۳۰ ، $F = \langle x_1 \rangle \cong \mathbf{Z}$ و $G = \langle d_1x_1 \rangle \cong \mathbf{Z}$ $(d_i \in \mathbf{N}^*)$. به استقرا عمل کرده ، فرض می‌کنیم قضیه برای تمام گروههای آبلی آزاد با رتبهٔ کمتر از n درست باشد . همچنین ، S مجموعهٔ

تمام اعداد صحیح s باشد به‌طوری‌که پایه‌ای مانند $\{y_1, \ldots, y_n\}$ از F و عنصری در G به شکل $(k_i \in \mathbf{Z})\ sy_1 + k_2y_2 + \cdots + k_ny_n$ موجود باشد. توجه کنید که در این حالت $\{y_2, y_1, y_3, \ldots, y_n\}$ نیز پایه‌ای از F است، که از آنجا $k_2 \in S$؛ به‌همین نحو، به‌ازای $j = 3,4, \ldots, n$ ، $k_j \in S$. چون $G \neq 0$ ، داریم $S \neq \varnothing$. از اینرو، S شامل دست کم یک عدد صحیح مثبت مانند d_1 است و به‌ازای پایه‌ای مانند $\{y_1, \ldots, y_n\}$ از F ، $v \in G$ ای وجود دارد به‌طوری‌که $v = d_1y_1 + k_2y_2 + \cdots + k_ny_n$. بنابر الگوریتم تقسیم، به‌ازای هر $i = 2, \ldots, n$ ، $k_i = d_1q_i + r_i$ که در آن $0 \leq r_i < d_1$ ، که از آنجا

$$v = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n.$$

فرض کنیم $W = \{x_1, y_2, \ldots, y_n\}$ ، $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. در این صورت، طبق لم ۵.۱، W یک پایهٔ F است. چون $v \in G$ ، $r_i < d_1$ و با هر ترتیب یک پایه از F است، مینیمالی d_1 در S ایجاب می‌کند که $r_2 = r_3 = \cdots = r_n = 0$ ؛ و درنتیجه، $d_1x_1 = v \in G$.

فرض کنیم $H = \langle y_2, y_3, \ldots, y_n \rangle$. پس H گروه‌آبلی آزادی از رتبهٔ $n - 1$ است به طوری‌که $F = \langle x_1 \rangle \oplus H$. به علاوه، حکم می‌کنیم که $G = \langle v \rangle \oplus (G \cap H) = \langle d_1x_1 \rangle \oplus (G \cap H)$. چون $\{x_1, y_2, \ldots, y_n\}$ پایه‌ای از F است، $\langle v \rangle \cap (G \cap H) = 0$. هرگاه $(t_i \in \mathbf{Z})u = t_1x_1 + t_2y_2 + \cdots + t_ny_n \in G$ ، آنگاه، طبق الگوریتم تقسیم، $t_1 = d_1q_1 + r_1$ ، که در آن $0 \leq r_1 < d_1$. لذا، G شامل $u - q_1v = r_1x_1 + t_2y_2 + \cdots + t_ny_n$ است. مینیمالی d_1 در S ایجاب می‌کند که $r_1 = 0$ ، که از آنجا $t_2y_2 + \cdots + t_ny_n \in G \cap H$ و $u = q_1v + (t_2y_2 + \cdots + t_ny_n)$. از اینرو، $G = \langle v \rangle + (G \cap H)$ ، که حکم ما را ثابت می‌کند (تعریف ۸.۸.۱).

یا $G \cap H = 0$ ، که در این حالت $G = \langle d_1x_1 \rangle$ و قضیه درست است، یا $G \cap H \neq 0$. پس، طبق فرض استقرا، پایه‌ای مانند $\{x_2, x_3, \ldots, x_n\}$ از H و اعداد صحیح مثبتی مانند $r, d_2, d_3, \ldots, d_r$ وجود دارند به‌طوری‌که $d_r \mid \cdots \mid d_3 \mid d_2$ و $G \cap H$ آبلی آزاد با پایهٔ $\{d_2x_2, \ldots, d_rx_r\}$ است. چون $F = \langle x_1 \rangle \oplus H$ و $G = \langle d_1x_1 \rangle \oplus (G \cap H)$ ، به آسانی معلوم می‌شود که $\{x_1, x_2, \ldots, x_n\}$ پایه‌ای از F و $\{d_1x_1, \ldots, d_rx_r\}$ پایه‌ای از G است. برای اتمام مرحلهٔ استقرایی برهان، کافی است نشان دهیم که $d_1 \mid d_2$. بنابر الگوریتم تقسیم، $d_2 = qd_1 + r_0$ ، که در آن $0 \leq r_0 < d_1$. چون بنابر لم ۵.۱ $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ یک پایهٔ F است و

$$r_0x_2 + d_1(x_1 + qx_2) = d_1x_1 + d_2x_2 \in G$$

مینیمالی d_i در S ایجاب می‌کند که $r_0 = 0$ ، که از آنجا $d_1 \mid d_2$.

نتیجهٔ ۷.۱ . هرگاه G یک گروه آبلی با تولید متناهی باشد که به وسیلهٔ n عنصر تولید شده‌است ، آنگاه هر زیرگروه H از G را می‌توان با m عنصر که $m \leq n$ تولید کرد .

این نتیجه در صورت حذف کلمهٔ آبلی درست نیست (تمرین ۸) .

برهان ۷.۱ . طبق قضیهٔ ۴.۱ ، یک گروه آبلی آزاد مانند F از رتبهٔ n و یک برویختی مانند $\pi : F \to G$ وجود دارد . $\pi^{-1}(H)$ زیرگروه F است ؛ ولذا ، طبق قضیهٔ ۶.۱ ، آزاد واز رتبهٔ $m \leq n$ است . نقش هر پایهٔ $\pi^{-1}(H)$ تحت π مجموعه‌ای‌است مرکب از حداکثر m عنصر که $\pi(\pi^{-1}(H)) = H$ را تولید می‌کند .

تمرینات

۱ . (آ) هرگاه G گروهی آبلی بوده و $m \in \mathbf{Z}$ ، آنگاه $mG = \{mu \mid u \in G\}$ زیرگروهی از G است .

(ب) هرگاه $G \cong \sum_{i \in I} G_i$ ، آنگاه $mG \cong \sum_{i \in I} mG_i$ و $G/mG \cong \sum_{i \in I} G_i/mG_i$.

۲ . گویند زیرمجموعهٔ X از گروه‌آبلی F **مستقل خطی** است اگر $n_1x_1 + \cdots + n_kx_k = 0$ همواره‌ایجاب‌کند که به‌ازای هر i ، $n_i = 0$ (که در آن $n_i \in \mathbf{Z}$ و $x_1, \ldots, x_k$ عناصر متمایزی از X اند) .

(آ) X مستقل خطی است اگر و فقط‌اگر هر عنصر ناصفر زیرگروه $\langle X \rangle$ را بتوان به طور منحصر به فرد به شکل $n_1x_1 + \cdots + n_kx_k$ نوشت ($n_i \in \mathbf{Z}$ ، $n_i \neq 0$ ، و $x_1, \ldots, x_k$ عناصر متمایزی از X اند) .

(ب) اگر F آبلی‌آزادازرتبهٔ متناهی n باشد ، درست نیست که هر زیرمجموعهٔ مستقل خطی از n عنصر یک پایه است [**راهنمایی .** $F = \mathbf{Z}$ را در نظر بگیرید] .

(پ) اگر F آبلی آزاد باشد ، درست نیست که هر زیرمجموعهٔ مستقل خطی F را می‌توان به پایه‌ای از F وسعت داد .

(ت) اگر F آبلی آزاد باشد ، درست نیست که هر مجموعهٔ مولد F شامل پایه‌ای

از F است. امـا، اگـر F با تولید متناهی به وسیلهٔ n عنصر باشد، F از رتبهٔ $m \leq n$ می‌باشد.

۳. فرض کنید $X = \{a_i \mid i \in I\}$ یک مجموعه باشد. گروه آبلی آزاد بر X مساوی (یکریخت با) گروه تعریف‌شده با مولدهای X و روابط (در نماد ضربی) $\{a_i a_j a_i^{-1} a_j^{-1} = e \mid i,j \in I\}$ است.

۴. یک گروه آبلی آزاد گروهی آزاد است (بخش ۱ . ۹) اگر و فقط اگر دوری باشد.

۵. مجموع مستقیم خانـواده‌ای از گـروههای آبلی آزاد یک گروه آبلی آزاد اسـت. (حاصل‌ضرب مستقیم گروههای آبلی آزاد لزوماً آبلی آزاد نیست؛ ر.ک. ال. فوکس[1] [۱۳، ص ۱۶۸].)

۶. هرگاه $F = \sum_{x \in X} \mathbf{Z}x$ یک گروه آبلی آزاد بوده، و G زیرگروهی با پایهٔ $X' = X - \{x_0\}$ به‌ازای $x_0 \in X$ می‌باشد، آنگاه $F/G \cong \mathbf{Z}x_0$. این نتیجه را به زیرمجموعه‌های دلخواه X' از X تعمیم دهید.

۷. هر گـروه آبلی آزاد نـاصفر، به‌ازای هر عدد صحیح مثبت n، دارای زیرگروهی با اندیس n است.

۸. فرض کنید G گروه ضـربی تولید شده به وسیلهٔ ماتریسهای حقیقی $a = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ و $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ باشد. هرگاه H مجموعهٔ تمام ماتریسهایی در G باشد که درایه‌های قطر (اصلی) آنها ۱ اند، آنگاه H زیرگروهی است اما نه با تولید متناهی.

۹. فرض کنید G گروهی آبلی با تولید متناهی باشد که در آن هیچ عنصری (جز 0) مرتبهٔ متنـاهی ندارد. دراین‌صورت، G یک گروه آبلی آزاد است. [**راهنمایی.** قضیهٔ ۱ . ۶ .]

۱۰. (آ) نشان دهید که گروه جمعی اعداد گویای $\mathbf{Q}$ با تولید متناهی نیست.

(ب) نشان دهید که $\mathbf{Q}$ آزاد نیست.

(پ) نتیجه بگیرید کـه تمرین ۹ درصورت حذف فرض "با تولید متناهی" درست نیست.

---

[1] L. Fuchs

۱۱ . (آ) فرض کنید G گروه جمعی تمام چند جمله‌ایها از x با ضرایب صحیح باشد. نشان دهید که G با گروه Q^* تمام اعداد گویای مثبت (تحت ضرب) یکریخت است. [**راهنمایی.** با استفاده از قضیهٔ اساسی حساب، یک یکریختی بسازید.]

(ب) گروه Q^* آبلی آزاد است با پایهٔ $\{p\}$ [p در $\mathbf{Z}$ اول است].

۱۲ . فرض کنید F گروه‌آزاد (نه‌لزوما "آبلی") بر مجموعهٔ X باشد (مثل بخش I ۹ . ۱) و G گروه آزاد بر مجموعهٔ Y باشد. همچنین، F' زیرگروهی از F باشد که به وسیلهٔ $\{aba^{-1}b^{-1} | a,b \in F\}$ تولید شده است؛ و به همین نحو، در مورد G'.

(آ) $F' \lhd F$ ، $G' \lhd G$ ، و $F/F', G/G'$ آبلی‌اند [ر.ک. قضیهٔ ۸ . ۷ در زیر].

(ب) F/F' [G/G'] یک گروه آبلی آزاد از رتبهٔ $|X|$ [$|Y|$] است.

[**راهنمایی.** $\{xF' | x \in X\}$ یک پایهٔ F/F' است.]

(پ) $F \cong G$ اگر و فقط اگر $|X| = |Y|$. [**راهنمایی.** هرگاه $\varphi : F \cong G$ ، آنگاه φ یک یکریختی مانند $F/F' \cong G/G'$ القا می‌کند. حکم ۳ . ۱ و قسمت (ب) را به کار برید. عکس مطلب قضیهٔ I ۷ . ۸ است.]

۲ گروههای آبلی با تولید متناهی

بحث را با اثبات دو قضیهٔ ساختاری مختلف برای گروههای آبلی با تولید متناهی آغاز می‌کنیم. سپس قضیهٔ یکتایی (۶ . ۲) نشان می‌دهد که هر قضیهٔ ساختاری مجموعه‌ای از پایاهای عددی برای یک گروه به دست می‌دهد (یعنی، دو گروه دارای پایاهای یکسانند اگر و فقط اگر یکریخت باشند). لذا، هر قضیهٔ ساختاری به رده‌بندی کامل (با تقریب یکریختی) تمام گروههای آبلی با تولید متناهی منجر می‌شود. مانند بخش ۱، ***تمام گروهها به‌طور جمعی نوشته می‌شوند.*** بسیاری از نتایج این بخش (ولی نه برهانهای آنها) را می‌توان به گروههایی آبلی که با تولید متناهی نیستند تعمیم داد؛ ر.ک. ال، فوکس [۱۳] یا آی. کاپلانسکی[1] [۱۷].

تمام قضایای ساختاری اثبات شده در اینجا حالات خاصی هستند از قضایای نظیر برای مدولهای با تولید متناهی روی یک دامنهٔ ایده‌آل اصلی (بخش IV ۶ . ۰). بعضی از خوانندگان ممکن است روش اثبات به کار رفته در بخش IV ۶ . را به روش استفاده شده در اینجا، که قویا" به قضیهٔ ۱ . ۶ وابسته است، ترجیح دهند.

1. I.Kaplansky

قضیهٔ ۱۰۲ . *هر گروه آبلی با تولید متناهی G مساوی (یکریخت با) مجموع مستقیمی از گروههای دوری است که در آن جمعوندهای دوری متناهی (در صورت وجود) از مراتب $m_1, \ldots, m_t$ اند که $m_1 > 1$ و $m_1 \mid m_2 \mid \cdots \mid m_t$.*

برهان . هرگاه $G \neq 0$ و G با n عنصر تولید شده باشد، آنگاه، طبق قضیهٔ ۴۰۱، گروه آبلی آزادی مانند F از رتبهٔ n و بروریختیی مانند $\pi : F \to G$ وجود دارد. هرگاه π یک یکریختی باشد، آنگاه (n جمعوند) $G \cong F \cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$. در غیر این صورت، طبق قضیهٔ ۶۰۱، پایه‌ای مانند $\{x_1, \ldots, x_n\}$ از F و اعداد صحیح مثبتی مانند $d_1, \ldots, d_r$ وجوددارند به طوری که $1 \leq r \leq n$، $d_1 \mid d_2 \mid \cdots \mid d_r$، و $\{d_1x_1, \ldots, d_rx_r\}$ پایه‌ای از $K = \operatorname{Ker} \pi$ است. اما $F = \sum_{i=1}^{n} \langle x_i \rangle$ و $K = \sum_{i=1}^{r} \langle d_i x_i \rangle$ ، که در آن $\langle x_i \rangle \cong \mathbf{Z}$ و، تحت همان یکریختی، $\langle d_i x_i \rangle \cong d_i\mathbf{Z} = \{d_i u \mid u \in \mathbf{Z}\}$. به‌ازای $i = r+1, r+2, \ldots, n$، فرض می‌کنیم $d_i = 0$ ؛ درنتیجه، $K = \sum_{i=1}^{n} \langle d_i x_i \rangle$. پس، طبق نتایج I ۷۰۵ ، I ۸۰۵ ، و I ۱۱۰۸ ،

$$G \cong F/K = \sum_{i=1}^{n} \langle x_i \rangle \Big/ \sum_{i=1}^{n} \langle d_i x_i \rangle \cong \sum_{i=1}^{n} \langle x_i \rangle / \langle d_i x_i \rangle \cong \sum_{i=1}^{n} \mathbf{Z}/d_i\mathbf{Z}.$$

هرگاه $d_i = 1$ ، آنگاه $\mathbf{Z}/d_i\mathbf{Z} = \mathbf{Z}/\mathbf{Z} = 0$ ؛ هرگاه $d_i > 1$ ، آنگاه $\mathbf{Z}/d_i\mathbf{Z} \cong Z_{d_i}$ ؛ هرگاه $d_i = 0$ ، آنگاه $\mathbf{Z}/d_i\mathbf{Z} = \mathbf{Z}/0 \cong \mathbf{Z}$. فرض کنیم $m_1, \ldots, m_t$ (به ترتیب) آن d_i هایی باشند که $d_i \neq 0, 1$ ، و s تعداد d_i هایی باشد که $d_i = 0$. دراین‌صورت،

$$G \cong Z_{m_1} \oplus \cdots \oplus Z_{m_t} \oplus (\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}),$$

که در آن $m_1 > 1$ ، $m_1 \mid m_2 \mid \cdots \mid m_t$ ، و $(\mathbf{Z} \oplus \cdots \oplus \mathbf{Z})$ از رتبهٔ s است.

قضیهٔ ۲۰۲ . *هر گروه آبلی با تولید متناهی G مساوی (یکریخت با) مجموع مستقیم متناهی گروههایی دوری است که هر یک نامتناهی یا از مرتبهٔ توانی از یک عدد اول است.*

طرح برهان . قضیه نتیجهٔ فوری قضیهٔ ۱۰۲ و لم زیر است. برهانی دیگر در تمرین ۴ به‌اختصار آمده است.

لم ۳۰۲ . *هرگاه* m *عدد صحیح مثبتی بوده و* $m = p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ ($p_1, \ldots, p_t$ *اعداد اولی متمایز بوده و هر* $n_i > 0$)، *آنگاه* $Z_m \cong Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_t^{n_t}}$.

طرح برهان . از استقرا بر تعداد t اعداد اول در تجزیهٔ m به عوامل اول و نیز اینکه

$$\text{هر وقت } (r,n) = 1 \text{ ، } Z_{rn} \cong Z_r \oplus Z_n$$

که اینک بـه اثبات آن می‌پردازیم استفاده کنید . عنصر $n = n1 \in Z_{rn}$ از مرتبهٔ r است (قضیهٔ ۴۰۳ . I (هفت))، که از آنجا $Z_r \cong \langle n1 \rangle < Z_{rn}$ و نگاشت $\psi_1 : Z_r \to Z_{rn}$ داده شده با $k \mapsto nk$ یک تکریختی است . بـه همین نحو، نگاشت $\psi_2 : Z_n \to Z_{rn}$ داده شده با $k \mapsto rk$ یک تکریختی است . طبـق برهان قضیهٔ ۵۰۸ . I ، نگاشت $\psi : Z_r \oplus Z_n \to Z_{rn}$ داده شده با $(x,y) \mapsto \psi_1(x) + \psi_2(y) = nx + ry$ یک همـریختی تعـریف شـده است . چون $(r,n) = 1$ ، بـه‌ازای $a,b \in Z$ ای ، $ra + nb = 1$ (آشنایی ،قضیهٔ ۵۰۶) . از اینرو، بـه‌ازای هـر $k \in Z_{rn}$ ، $k = rak + nbk = \psi(bk,ak)$ و ψ یـک بـروریختی است . چـون $|Z_r \oplus Z_n| = rn = |Z_{rn}|$ ، ψ نیز باید تکریختی باشد .

نتیجهٔ ۴۰۲ . *هرگاه* G *یک‌گروه آبلی متناهی از مرتبهٔ* n *باشد ، آنگاه ، به‌ازای هر عدد صحیح مثبت* m *که* n *را عاد می‌کند ،* G *زیرگروهی از مرتبهٔ* m *دارد .*

طرح برهان . از قضیهٔ ۲۰۲ استفاده کنید و ملاحظه کنید که $G \cong \sum_{i=1}^{k} G_i$ ایجاب می‌کند که $|G| = |G_1||G_2|\cdots|G_k|$ و، بنابر لم ۵۰۲ (پنج) زیر ، به‌ازای $i \leq r$ ، $p^{r-i}Z_{p^r} \cong Z_{p^i}$.

تبصره . نتیجهٔ ۴۰۲ در صورت آبلی نبـودن G ممکن است درست نباشد (تمرین ۸۰۶ . I) .

در قضیهٔ ۶۰۲ درزیر نشان خواهیم داد که مراتب جمعوندهای دوری در تجزیه‌های قضایای ۱۰۲ و ۲۰۲ درواقـع بـه‌طور منحصـر به فرد با گروه G معین می‌شوند . ابتدا به جمع‌آوری مـطالبی گونـاگون در بـاب گروههای آبلی که در برهان به کار خواهند رفت می‌پردازیم .

لم ۵۰۲ . فرض کنیم G گروهی آبلی ، m عددی صحیح ، و p عدد صحیح اولی باشد . دراین‌صورت ، هر یک از مجموعه‌های زیر زیرگروهی از G است :

(یک) $mG = \{mu \mid u \in G\}$ ؛

(دو) $G[m] = \{u \in G \mid mu = 0\}$ ؛

(سه) $G(p) = \{u \in G \mid |u| = p^n$ ، به‌ازای $n \geq 0\}$ ؛

(چهار) $G_t = \{u \in G \mid |u|$ متناهی است $\}$.

بخصوص ، یکریختیهای زیر وجود دارند :

(پنج) $p^m Z_{p^n} \cong Z_{p^{n-m}}$ $(m < n)$ و $Z_{p^n}[p] \cong Z_p$ $(n \geq 1)$.

فرض کنیم H و G_i $(i \in I)$ گروههایی آبلی باشند .

(شش) هرگاه $g : G \to \sum_{i \in I} G_i$ یکریختی باشد ، آنگاه تحدیدهای g به ترتیب به mG و $G[m]$ یکریختیهای $G[m] \cong \sum_{i \in I} G_i[m]$ و $mG \cong \sum_{i \in I} mG_i$ می‌باشند .

(هفت) هرگاه $f : G \to H$ یکریختی باشد ، آنگاه تحدیدهای f به ترتیب به G_t و $G(p)$ یکریختیهای $G_t \cong H_t$ و $G(p) \cong H(p)$ می‌باشند .

طرح برهان . (یک) تا (چهار) تمرین‌اند ؛ فرض آبلی بودن G اساسی است (S_3 مثالهای نقض برای (یک) تا (سه) ، و تمرین I . ۵۰۳ برای (چهار) به دست می‌دهد). (پنج) بنابر قضیهٔ I . ۴۰۳ ، $p^{n-1} \in Z_{p^n}$ از مرتبهٔ p است ، که از آنجا $\langle p^{n-1} \rangle \cong Z_p$ و $\langle p^{n-1} \rangle < Z_{p^n}[p]$. هرگاه $u \in Z_{p^n}[p]$ ، آنگاه در Z_{p^n} ، $pu = 0$ ؛ در نتیجه ، در $\mathbf{Z}$ ، $pu \equiv 0 \pmod{p^n}$. اما $p^n \mid pu$ ایجاب می‌کند که $p^{n-1} \mid u$. لذا ، در Z_{p^n} ، $u \in \langle p^{n-1} \rangle$ و $Z_{p^n}[p] < \langle p^{n-1} \rangle$. برای حکم دوم توجه کنید که ، طبق قضیهٔ I . ۴۰۳ (هفت) ، $p^m \in Z_{p^n}$ از مرتبهٔ p^{n-m} است . بنابراین ، $p^m Z_{p^n} = \langle p^m \rangle \cong Z_{p^{n-m}}$. (شش) تمرین است . (هفت) هرگاه $f : G \to H$ یک همریختی بوده و $x \in G(p)$ از مرتبهٔ p^n باشد ، آنگاه $p^n f(x) = f(p^n x) = f(0) = 0$. لذا ، $f(x) \in H(p)$. از اینرو ، $f : G(p) \to H(p)$. هرگاه f یکریختی باشد ، آنگاه همین استدلال نشان می‌دهد که $f^{-1} : H(p) \to G(p)$. چون $ff^{-1} = 1_{H(p)}$ و $f^{-1}f = 1_{G(p)}$ ، $G(p) \cong H(p)$. قسمت دیگر (هفت) به همین نحو ثابت می‌شود .

هرگاه G گروهی آبلی باشد، آنگاه زیرگروه G_t تعریف شده در لم ۵۰۲ . **زیرگروه تابی** G نام دارد. هرگاه $G = G_t$ ، آنگاه گوییم G یک **گروه تابی** است. هرگاه $G_t = 0$ ، آنگاه گوییم G **فارغ از تاب** است. برای رده‌بندی کاملی از تمام گروههای تابی شمارشپذیر، ر.ک. آی. کاپلانسکی [۱۷] .

قضیهٔ ۶۰۲ . *فرض کنیم G یک گروه آبلی با تولید متناهی باشد.*
(یک) عدد صحیح نامنفی منحصر به فردی مانند s هست به‌طوری‌که تعداد جمعوندهای دوری نامتناهی در هر تجزیهٔ G به صورت مجموع مستقیمی از گروههای دوری دقیقا " s است.
(دو) یا G آبلی آزاد است یا اعداد صحیح مثبت و منحصر به فردی (نه لزوما " متمایز) مانند $m_1, \ldots, m_t$ وجود دارند به‌طوری‌که $m_1 > 1$ ، $m_1 \mid m_2 \mid \cdots \mid m_t$ و

$$G \cong Z_{m_1} \oplus \cdots \oplus Z_{m_t} \oplus F$$

که در آن F آبلی آزاد است.
(سه) یا G آبلی آزاد است یا اعداد صحیح مثبتی مانند $p_1^{a_1}, \ldots, p_k^{a_k}$ که صرف‌نظر از ترتیب اعضا منحصر به فردند، موجود می‌باشند به‌طوری‌که $p_1, \ldots, p_k$ اعدادی اول (نه لزوما " متمایز) و $s_1, \ldots, s_k$ اعدادی صحیح و مثبت (نه لزوما " متمایز) بوده، و

$$G \cong Z_{p_1^{a_1}} \oplus \cdots \oplus Z_{p_k^{a_k}} \oplus F$$

که در آن F آبلی آزاد است.

برهان . (یک) هر تجزیهٔ G به صورت مجموعی مستقیم از گروههای دوری (که، طبق قضیهٔ ۱۰۲ ، دست‌کم یکی وجود دارد) یک یکریختی $G \cong H \oplus F$ به دست می‌دهد، که در آن H مجموع مستقیمی (احتمالا "0") از گروههای دوری متناهی بوده و F یک گروه آبلی آزاد است که رتبه‌اش دقیقا " با تعداد جمعوندهای دوری نامتناهی در تجزیه، یعنی s ، مساوی می‌باشد. هرگاه $\iota : H \to H \oplus F$ انژکسیون کانونی $(h \mapsto (h,0))$ باشد، آنگاه $\iota(H)$ بوضوح زیرگروه تابی $H \oplus F$ است. بنابر لم ۵۰۲ ، تحت یکریختی $G \cong H \oplus F$ داریم $G_t \cong \iota(H)$. لذا، طبق نتیجهٔ ۸۰۵ . I ، $G/G_t \cong (F \oplus H)/\iota(H) \cong F$.

بنابراین، هر تجزیهٔ G منجر به این می‌شود که G/G_t یک گروه آبلی آزاد است که رتبه‌اش با تعداد جمعوندهای دوری نامتناهی در تجزیه، یعنی s، مساوی می‌باشد. چون G/G_t به تجزیهٔ خاصی وابسته نیست و رتبهٔ G/G_t، بنابرقضیهٔ ۲۰۱، پایاست، پس s به‌طور منحصر به فرد معین می‌شود.

(سه) فرض کنیم G دو تجزیه داشته باشد، مثلا"،

$$G \cong \sum_{i=1}^{r} Z_{n_i} \oplus F \quad \text{و} \quad G = \sum_{j=1}^{d} Z_{k_j} \oplus F' ،$$

که در آن هریک از n_i, k_j توانی از عددی اول (ممکن است اعداد اول متمایز باشند) بوده و F, F' آبلی آزادند (طبق قضیهٔ ۲۰۲، دست‌کم یک‌چنین تجزیه‌ای وجود دارد). باید نشان دهیم که $r = d$ و (پس از ترتیب مجدد)، به‌ازای هر i، $n_i = k_i$. به آسانی دیده می‌شود که زیرگروه تابی $\sum Z_{n_i} \oplus F$ مساوی (یکریخت با) $\sum Z_{n_i}$ است و به همین نحو در مورد تجزیهٔ دیگر. از اینرو، بنابر لم ۵۰۲، $\sum_{i=1}^{r} Z_{n_i} \cong G_t \cong \sum_{j=1}^{d} Z_{k_j}$. به‌ازای هر عدد اول p، $(\sum Z_{n_i})(p)$ بوضوح مساوی (یکریخت با) مجموع مستقیم آن Z_{n_i} هایی است که n_i توانی از p است و به همین نحو در مورد تجزیهٔ دیگر. چون، طبق لم ۵۰۲، به‌ازای هر p اول $(\sum Z_{n_i})(p) \cong (\sum Z_{k_i})(p)$، کافی است فرض شود که $G = G_t$ و هر n_i, k_i توانی از عدد اول ثابت p اند (درنتیجه، $G = G(p)$). از اینرو، داریم

$$\sum_{i=1}^{r} Z_{p^{a_i}} \cong G \cong \sum_{j=1}^{d} Z_{p^{c_j}} (1 \le a_1 \le a_2 \le \cdots \le a_r;\ 1 \le c_1 \le c_2 \le \cdots \le c_d).$$

ابتدا نشان می‌دهیم که در هر دو تجزیهٔ یک گروه از این نوع باید داشته باشیم $r = d$. لم ۵۰۲ و تجزیهٔ اول G نشان می‌دهند که

$$G[p] \cong \sum_{i=1}^{r} Z_{p^{a_i}}[p] \cong Z_p \oplus \cdots \oplus Z_p \quad (r \text{ جمعوند})$$

که از آنجا $|G[p]| = p^r$. استدلالی مشابه با تجزیهٔ دوم نشان می‌دهد که $|G[p]| = p^d$. بنابراین، $p^r = p^d$ و $r = d$.

فرض کنیم ν $(1 \le \nu \le r)$ اولین عدد صحیحی باشد که به‌ازای هر $i < \nu$، $a_i = c_i$ و $a_\nu \neq c_\nu$. می‌توان فرض کرد $a_\nu < c_\nu$. چون به ازای $a_i \le a_\nu$، $p^{a_\nu} Z_{p^{a_i}} = 0$، تجزیهٔ اول و لم ۵۰۲ ایجاب می‌کنند که

$$p^{a_v}G \cong \sum_{i=1}^{r} p^{a_v}Z_{p^{a_i}} \cong \sum_{i=v+1}^{r} Z_{p^{a_i-a_v}},$$

که در آن $a_{v+1}-a_v \leq a_{v+2}-a_v \leq \cdots \leq a_r-a_v$. واضح است که حداکثر $r-(v+1)+1 = r-v$ جمعوند ناصفر وجود دارد . به همین نحو ، چون به‌ازای $i<v$ ، $a_i = c_i$ و $a_v < c_v$ ، تجزیهٔ دوم ایجاب می‌کند که

$$p^{a_v}G \cong \sum_{i=v}^{r} Z_{p^{c_i-a_v}},$$

که در آن $1 \leq c_v-a_v \leq c_{v+1}-a_v \leq \cdots \leq c_r-a_v$. واضح است که دستکم $r-v+1$ جمعوند ناصفر وجود دارند . بنابراین ، دو تجزیه از گروه $p^{a_v}G$ به صورت مجموع مستقیم گروههای دوری از مرتبهٔ توان اول داریم و تعداد جمعوندهای تجزیهٔ اول از تعداد جمعوندهای تجزیهٔ دوم کمتر است . این با بخشی از قضیه که در بند قبل ثابت شد (و در اینجا بر $p^{a_v}G$ اعمال گشت) متناقض است . لذا ، باید به‌ازای هر i داشته باشیم $a_i = c_i$.

(دو) فرض کنیم G دو تجزیه داشته باشد ؛ مثلا" ،

$$G \cong Z_{k_1} \oplus \cdots \oplus Z_{k_d} \oplus F' \quad \text{و} \quad G \cong Z_{m_1} \oplus \cdots \oplus Z_{m_t} \oplus F$$

که در آنها $m_1 > 1, m_1 \mid m_2 \mid \cdots \mid m_t, k_1 > 1, k_1 \mid k_2 \mid \cdots \mid k_d$ و F, F' گروههای آبلی آزادند ؛ (این‌گونه تجزیه طبق قضیهٔ ۱۰۲ وجود دارد) . هر m_i, k_j دارای تجزیه به اعداد اول است و ، با وارد کردن عواملی به شکل p^0 ، می‌توان فرض کرد که اعداد اول (متمایز) $p_1, \ldots, p_r$ در تمام تجزیه‌ها می‌آیند ؛ مثلا" ،

$$\begin{aligned} m_1 &= p_1^{a_{11}}p_2^{a_{12}}\cdots p_r^{a_{1r}} & k_1 &= p_1^{c_{11}}p_2^{c_{12}}\cdots p_r^{c_{1r}} \\ m_2 &= p_1^{a_{21}}p_2^{a_{22}}\cdots p_r^{a_{2r}} & k_2 &= p_1^{c_{21}}p_2^{c_{22}}\cdots p_r^{c_{2r}} \\ &\vdots & &\vdots \\ m_t &= p_1^{a_{t1}}p_2^{a_{t2}}\cdots p_r^{a_{tr}} & k_d &= p_1^{c_{d1}}p_2^{c_{d2}}\cdots p_r^{c_{dr}}. \end{aligned}$$

چون $m_1 \mid m_2 \mid \cdots \mid m_t$ ، باید به‌ازای هر j داشته باشیم $0 \leq a_{1j} \leq a_{2j} \leq \cdots \leq a_{tj}$ به همین نحو ، به‌ازای هر j ، $0 \leq c_{1j} \leq c_{2j} \leq \cdots \leq c_{dj}$. بنابر لمهای ۳۰۲ و ۵۰۲ ،

$$\sum_{i,j} Z_{p_j^{a_{ij}}} \cong \sum_{i=1}^{t} Z_{m_i} \cong G_t \cong \sum_{i=1}^{d} Z_{k_i} \cong \sum_{i,j} Z_{p_j^{c_{ij}}},$$

که در آن بعضی از جمعوندها ممکن است صفر باشند . پس نتیجه می‌شود که به‌ازای هر $j = 1,2,\ldots,r$ ،

$$\sum_{i=1}^{t} Z_{p_j^{a_{ij}}} \cong G(p_j) \cong \sum_{i=1}^{d} Z_{p_j^{c_{ij}}}.$$

چون $m_1 > 1$ ، p_j ای موجود است به‌طوری که $a_{tj} \leq \cdots \leq a_{1j} \leq 1$ ؛ که درنتیجه $\sum_{i=1}^{t} Z_{p_j^{a_{ij}}}$ دارای t جمعوندناصفراست . بنابر (سه) ، $\sum_{i=1}^{d} Z_{p_j^{c_{ij}}}$ دقیقاً " t جمعوند ناصفر دارد ، که‌ازآنجا $t \leq d$. به همین نحو ، $k_1 > 1$ ایجاب می‌کند که $d \leq t$ ؛ و درنتیجه ، $d = t$. اما ، بنابر (سه) ، باید به‌ازای هر i,j ، $a_{ij} = c_{ij}$ ، که ایجاب می‌کند که به‌ازای $i = 1,2,\ldots,t$ ، $m_i = k_i$.

هرگاه G یک گروه آبلی با تولید متناهی باشد ، آنگاه اعداد صحیح منحصر به فرد $m_1,\ldots,m_t$ ، در قضیهٔ ۶.۲ (دو) ***عاملهای پایای*** G نامیده می‌شوند . توانهای اول منحصر به فرد در قضیهٔ ۶.۲ (سه) ***مقسوم‌علیه‌های مقدماتی*** G نام دارند .

نتیجهٔ ۷.۲ . دو گروه آبلی با تولیدمتناهی G و H ***یکریخت‌اند اگر وفقط اگر*** G/G_t و H/H_t ***دارای یک رتبه بوده و*** G و H ***عوامل پایا*** [***یا مقسوم‌علیه‌های مقدماتی***] ***یکسان داشته باشند .***

برهان . تمرین .

مثال . تمام گروههای آبلی متناهی از مرتبهٔ 1500 را می‌توان با تقریب یکریختی به صورت زیر معین کرد . چون حاصلضرب مقسوم علیه‌های مقدماتی گروه متناهی G باید مساوی $|G|$ باشد و $1500 = 2^2 \cdot 3 \cdot 5^3$ ، تنهاخانواده‌های ممکن از مقسوم علیه‌های مقدماتی عبارتند از $\{2,2,3,5^3\}$ ، $\{2,2,3,5,5^2\}$ ، $\{2,2,3,5,5,5\}$ ، $\{2^2,3,5^3\}$ ، $\{2^2,3,5,5^2\}$ ، و $\{2^2,3,5,5,5\}$. هر یک از این شش خانواده یک گروه آبلی از مرتبهٔ 1500 معین می‌کند (مثلا " ، $\{2,2,3,5^3\}$ گروه $Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_{125}$ رامعین می‌کند) . بنا بر قضیهٔ ۲.۲ ، هر گروه آبلی از مرتبهٔ 1500 با یکی از این شش گروه یکریخت است و ، طبق نتیجهٔ ۷.۲ ،

هیچ دو تا از این شش گروه با هم یکریخت نیستند .

هرگاه عاملهای پایای $m_1, \ldots, m_t$ گروه‌آبلی با تولید متناهی G معلوم باشند ، آنگاه برهان قضیهٔ ۶.۲ نشان می‌دهد که مقسوم‌علیه‌های مقدماتی G توانهای اول p^n $(n > 0)$ اند که در تجزیه‌های اول $m_1, \ldots, m_t$ ظاهر می‌شوند . به عکس ، اگر مقسوم‌علیه‌های مقدماتی G معلوم باشند ، آنها را می‌توان (پس از درج چند جمله به شکل p^0 در صورت لزوم) به صورت زیر مرتب نمود :

$$\begin{matrix} p_1^{n_{11}}, p_2^{n_{12}}, \ldots, p_r^{n_{1r}} \\ p_1^{n_{21}}, p_2^{n_{22}}, \ldots, p_r^{n_{2r}} \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ p_1^{n_{t1}}, p_2^{n_{t2}}, \ldots, p_r^{n_{tr}}. \end{matrix}$$

که در آن $p_1, \ldots, p_r$ اعداد اول متمایزی هستند ؛ به‌ازای هر $j = 1,2,\ldots,r$ و $n_{ij} \neq 0$ ای ، $n_{1j} \leq n_{2j} \leq \cdots \leq n_{tj}$ ؛ وبالاخره ، به‌ازای j ای ، $n_{1j} \neq 0$. طبق تعریف مقسوم‌علیه‌های مقدماتی (قضیهٔ ۶.۲ (سه)) ، $G \cong \sum_{i=1}^{t} \sum_{j=1}^{r} Z_{p_j^{n_{ij}}} \oplus F$ ، که در آن F آبلی آزاد است (و چند جمعوند 0 می‌باشد ، جمعوندهایی که در آنها $p_i^{n_{ij}} = p_i^0 = 1$) . به‌ازای هر $i = 1,2,\ldots,t$ ، قرار می‌دهیم $m_i = p_1^{n_{i1}} p_2^{n_{i2}} \cdots p_r^{n_{ir}}$ (یعنی ، m_i حاصلضرب سطر i م آرایهٔ فوق است) . چون $n_{1j} \neq 0$ ای ، $m_1 > 1$ و بنابر ساخت $m_1 \mid m_2 \mid \cdots \mid m_t$. طبق لم ۳.۲ ،

$$G \cong \sum_{i=1}^{t} \left(\sum_{j=1}^{r} Z_{p_j^{n_{ij}}} \right) \oplus F \cong \sum_{i=1}^{t} Z_{m_i} \oplus F$$

بنابر این ، طبق قضیهٔ ۶.۲ (دو) ، $m_1, \ldots, m_t$ عاملهای پایای G می‌باشند .

مثال . هرگاه G گروه $Z_5 \oplus Z_{15} \oplus Z_{25} \oplus Z_{36} \oplus Z_{54}$ باشد ، آنگاه ، بنابر لم ۳.۲ ،

$$G \cong Z_5 \oplus (Z_5 \oplus Z_3) \oplus Z_{25} \oplus (Z_9 \oplus Z_4) \oplus (Z_{27} \oplus Z_2)$$

لذا ، مقسوم‌علیه‌های مقدماتی G عبارتند از $2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$ ، که می‌توان آنها را به صورتی که در بالا توضیح دادیم مرتب کرد :

$$2^0,\ 3,\ 5$$
$$2,\ 3^2,\ 5$$
$$2^2,\ 3^3,\ 5^2.$$

درنتیجه، عاملهای‌پایای G عبارتنداز $1\cdot3\cdot5=15$ ، $2\cdot3^2\cdot5=90$ ،و $2^2\cdot3^3\cdot5^2=2700$ ؛ بنابراین، $G\cong Z_{15}\oplus Z_{90}\oplus Z_{2700}$.

مبحثی‌که‌طبعا "باید در این بخش مطرح شود تعیین ساختار یک گروه آبلی با تولید متناهی است که با مولدها و روابط توصیف شده است. اما، چون تکنیکهای ماتریسی احتمالا "بهترین‌راه‌پرداختن به این سوءالند، این مطلب در ضمیمهٔ بخش VII ۲۰ مطرح شده‌است. خوانندهٔ‌علاقه‌مندمی‌تواندآن را در وضع فعلی با کمی یا بدون مشکل بخواند.

تمرینات

۱. نشان‌دهیدکه‌یک گروه آبلی‌متناهی‌که دوری نباشد زیرگروهی دارد که با $Z_p\oplus Z_p$ ، به‌ازای عدد اولی مانند p ، یکریخت است.

۲. فرض‌کنید G یک گروه آبلی متناهی و x عنصری از مرتبهٔ ماکزیمال باشد. نشان دهید که $\langle x\rangle$ یک جمعوند مستقیم G است. با استفاده از این، برهان دیگری از قضیهٔ ۱۰۲ را به دست آورید.

۳. فرض‌کنید G یک p-گروه آبلی متناهی بوده (تمرین ۷) و $x\in G$ دارای مرتبهٔ ماکزیمال باشد. هرگاه $y\in G/\langle x\rangle$ دارای مرتبهٔ p^r باشد، آنگاه نماینده‌ای مانند $y\in G$ از هم مجموعهٔ y وجود دارد به طوری که $|y|=p^r$. [توجه کنید که هرگاه $|x|=p^t$ ، آنگاه $p^tG=0$.]

۴. با استفاده از تمرینهای ۳ و ۷، برهانی از قضیهٔ ۲۰۲ به دست آورید که از قضیهٔ ۱۰۲ مستقل باشد. [**راهنمایی.** اگر G یک p-گروه باشد، فرض‌کنید $x\in G$ مرتبهٔ ماکزیمال دارد؛ به استقرا، $G/\langle x\rangle$ مجموع مستقیم گروههایی دوری است، $G/\langle x\rangle=\langle\bar{x}_1\rangle\oplus\cdots\oplus\langle\bar{x}_n\rangle$ ، که در آن $|\bar{x}_i|=p^{r_i}$ و $1\le r_1\le r_2\le\cdots\le r_n$. نماینده‌های x_i از $\bar{x}_i$ را طوری اختیار کنید که $|x_i|=|\bar{x}_i|$. نشان دهید که $\langle x\rangle\oplus\langle x_1\rangle\oplus\cdots\oplus\langle x_n\rangle=G$ تجزیهٔ مطلوب است.]

۵. هرگاه G یک گروه آبلی با تولید متناهی باشد به‌طوری که G/G_t دارای رتبهٔ n

بوده، و H زیرگروهی از G باشد به‌طوری که H/H_t دارای رتبهٔ m است، آنگاه $m \leq n$ و $(G/H)/(G/H)_t$ دارای رتبهٔ $n - m$ می‌باشد.

۶. فرض کنید $k, m \in \mathbf{N}^*$. هرگاه $(k,m) = 1$، آنگاه $kZ_m = Z_m$ و $Z_m[k] = 0$. هرگاه $k \mid m$، مثلاً $m = kd$، آنگاه $kZ_m \cong Z_d$ و $Z_m[k] \cong Z_k$.

۷. یک (زیر) گروه که در آن مرتبهٔ هر عنصر توانی از عدد اول ثابت p باشد یک p-(زیر)گروه نامیده می‌شود (**تذکر.** $|0| = 1 = p^0$). فرض کنید G یک گروه تابی آبلی باشد.

(آ) $G(p)$، p-زیرگروه ماکزیمم منحصر به فرد G است (یعنی، هر p-زیرگروه G مشمول $G(p)$ است).

(ب) $G = \sum G(p)$، که در آن مجموع روی تمام اعداد اول p است به‌طوری که $G(p) \neq 0$. [**راهنمایی.** اگر $|u| = p_1^{n_1} \cdots p_t^{n_t}$، قرار می‌دهیم $m_i = |u|/p_i^{n_i}$. $c_i \in \mathbf{Z}$ ی وجود دارد به‌طوری که $c_1 m_1 + \cdots + c_t m_t = 1$، که از آنجا $u = c_1 m_1 u + \cdots + c_t m_t u$؛ ولی $c_i m_i u \in G(p_i)$.]

(پ) هرگاه H گروه تابی آبلی دیگری باشد، آنگاه $G \cong H$ اگر و فقط اگر به‌ازای جمیع p های اول، $G(p) \cong H(p)$.

۸. یک p گروه آبلی متناهی (تمرین ۷) به وسیلهٔ عناصر از مرتبهٔ ماکزیمال خود تولید می‌شود.

۹. گروه آبلی $Z_{p^3} \oplus Z_{p^2}$ چند زیرگروه از مرتبهٔ p^2 دارد؟

۱۰. (آ) فرض کنید G یک p-گروه آبلی متناهی باشد (تمرین ۷). نشان دهید که به‌ازای هر $n \geq 0$، $p^n G \cap G[p]$ یک زیرگروه $p^{n+1}G \cap G[p]$ است.

(ب) نشان دهید که $(p^n G \cap G[p])/(p^{n+1}G \cap G[p])$ مجموع مستقیمی از نسخه‌های Z_p است؛ فرض کنید k تعداد نسخه‌ها باشد.

(پ) G را به صورت مجموع مستقیمی از گروههای دوری بنویسید؛ نشان دهید که عدد k در قسمت (ب) تعداد جمعوندها از مرتبهٔ p^{n+1} می‌باشد.

۱۱. فرض کنید G، H، و K گروههایی آبلی با تولید متناهی باشند.

(آ) هرگاه $G \oplus G \cong H \oplus H$، آنگاه $G \cong H$.

(ب) هرگاه $G \oplus H \cong G \oplus K$، آنگاه $H \cong K$.

(پ) هرگاه G_1 یک گروه آبلی آزاد از رتبهٔ $\aleph_0$ باشد، آنگاه $G_1 \oplus \mathbf{Z} \oplus \mathbf{Z} \cong G_1 \oplus \mathbf{Z}$

ولی $\mathbf{Z} \oplus \mathbf{Z} \ncong \mathbf{Z}$.

تذکر. یک گروه آبلی فارغ از تاب شمارشپذیر با تولید نامتناهی مانند G وجود دارد به‌طوری که $G \cong G \oplus G \oplus G$ ولی $G \ncong G \oplus G$ ؛ درنتیجه، (آ) به‌ازای $H = G \oplus G$ برقرارنیست. ر.ک. ا. ال. اس. کورنر[1] [۶۰] . همچنین، ر.ک. تمرینات ۱۱.۳ ، ۱۲.۳ ، و IV . ۱۲.۳ .

۱۲ . (آ) مقسوم‌علیه‌های مقدماتی گروه $Z_2 \oplus Z_9 \oplus Z_{25}$ چه هستند؟ عاملهای پایای آن‌چه‌هستند ؟همین‌سوءال رادر مورد $Z_{26} \oplus Z_{42} \oplus Z_{49} \oplus Z_{200} \oplus Z_{1000}$ پاسخ‌دهید .

(ب) تمام گروههای آبلی از مرتبهٔ 64 را با تقریب یکریختی تعیین کنید ؛ همین کار را برای مرتبهٔ 96 انجام دهید .

(پ) تمام گروههای آبلی از مرتبهٔ n ، به‌ازای $n \leq 20$ ، را تعیین کنید .

۱۳ . نشان دهید که عاملهای پایای $Z_m \oplus Z_n$ عبارتند از (m,n) و $[m,n]$ (بزرگترین مقسوم‌علیه‌مشترک و کوچکترین مضرب مشترک) اگر $(m,n) > 1$ و mn اگر $(m,n) = 1$.

۱۴ . هرگاه H زیرگروهی از گروه‌آبلی متناهی G باشد ، آنگاه G زیرگروهی دارد که با G/H یکریخت است .

۱۵ . هر زیرگروه متناهی $\mathbf{Q}/\mathbf{Z}$ دوری است [ر.ک. تمرینهای I . ۷.۳ و ۷] .

۳ قضیهٔ کرول[2] ـ اشمیت[3]

گروههای $\mathbf{Z}$ و Z_{p^n} (p اول) تجزیه‌ناپذیرند ، بدین معنی که هیچیک مجموع مستقیم دو زیرگروه‌حقیقی‌خود نیست (تمرین I . ۱۰.۸) . درنتیجه، قضایای ۲.۲ و ۶.۲ (سه) را می‌توان‌چنین بیان‌کرد : هرگروه‌آبلی با تولید متناهی مجموع مستقیم تعدادی متناهی گروه تجزیه‌ناپذیر است و این جمعوندهای تجزیه‌ناپذیر با تقریب یکریختی به‌طور منحصر به فرد معین می‌شوند . حال این نتیجه را به ردهٔ وسیعی از گروهها (نه لزوما "آبلی") تعمیم می‌دهیم .[4]

تا پایان این فصل از نماد ضربی برای یک گروه دلخواه استفاده خواهیم کرد .

---

1. A.L.S. Corner
2. Krull
3. Schmidt
۴ . نتایج این بخش در بحثهای آتی مورد نیاز نیست .

تعریف ۱۰۳ . گروه G **تجزیه‌ناپذیر** است اگر $G \neq \langle e \rangle$ و G حاصلضرب مستقیم (داخلی) دو زیرگروه حقیقی خود نباشد .

لذا ، G تجزیه‌ناپذیر است اگر و فقط اگر $G \neq \langle e \rangle$ و $G \cong H \times K$ ایجاب کند که $H = \langle e \rangle$ یا $K = \langle e \rangle$ (تمرین ۱) .

چند مثال . هر گروه ساده (مثلا " ، $A_n, n \neq 4$) تجزیه‌ناپذیر است . اما گروههای تجزیه‌ناپذیر لزوما " ساده نیستند ؛ $\mathbf{Z}$ ، Z_{p^n} (p اول) ، و S_n تجزیه‌ناپذیرند ولی ساده نیستند (تمرینهای ۲ و I . ۱۰۸) .

تعریف ۲۰۳ . گوییم گروه G در **شرط زنجیر افزایشی** (ACC) بر زیرگروهها [نرمال] صدق می‌کند اگر به‌ازای هر زنجیر $G_1 < G_2 < \cdots$ از زیرگروههای [نرمال] G ، عدد صحیحی مانند n موجود باشد به‌طوری که به‌ازای هر $i \geq n$ ، $G_i = G_n$. گوییم G در **شرط زنجیر کاهشی** (DCC) بر زیرگروهها [نرمال] صدق می‌کند اگر به‌ازای هر زنجیر $G_1 > G_2 > \cdots$ از زیرگروههای [نرمال] G ، عدد صحیحی مانند n موجود باشد به‌طوری که به‌ازای هر $i \geq n$ ، $G_i = G_n$.

چند مثال . هر گروه متناهی در هر دو شرط زنجیری صدق می‌کند . $\mathbf{Z}$ در شرط زنجیر افزایشی صدق می‌کند ولی در شرط زنجیر کاهشی صدق نمی‌کند (تمرین ۵) و $Z(p^\infty)$ در شرط زنجیر کاهشی صدق می‌کند ولی در شرط زنجیر افزایشی صدق نمی‌کند (تمرین ۱۳) .

قضیهٔ ۳۰۳ . ***هرگاه گروه G در شرط زنجیر افزایشی یا کاهشی بر زیرگروههای نرمال صدق کند ، آنگاه G حاصلضرب مستقیم تعدادی متناهی زیرگروه تجزیه‌ناپذیر است .***

طرح برهان . فرض کنیم G حاصلضرب مستقیم تعدادی متناهی از زیرگروههای تجزیه‌ناپذیر نباشد . همچنین ، S مجموعهٔ تمام زیرگروههای نرمال H از G باشد به‌طوری که H یک عامل مستقیم G است (یعنی ، به‌ازای زیرگروهی از G مانند T_H ، $G = H \times T_H$) و H حاصلضرب مستقیم تعدادی متناهی از زیرگروههای تجزیه‌ناپذیر نباشد . واضح است که

$G \in S$. هرگاه $H \in S$ ، آنگاه H تجزیه‌ناپذیر است ، که از آنجا باید زیرگروههایی حقیقی مانند K_H و J_H از H موجودباشند به‌طوری که $H = K_H \times J_H \ (= J_H \times K_H)$. به علاوه ،یکی ازاین گروهها ، مثلا" ، K_H ، باید در S واقع باشد (بخصوص، بنابر تمرین I . ۱۲۰۸ ، K_H در G نرمال است) . فرض کنیم نگاشت $f: S \to S$ با $f(H) = K_H$ تعریف شده باشد . طبق قضیهٔ بازگشتی ۲۰۶ آشنایی (با $f_n = f$ به‌ازای هر n) تابعی مانند $\varphi : \mathbf{N} \to S$ وجود دارد به‌طوری که

$$\varphi(0) = G \quad \text{و} \quad \varphi(n+1) = f(\varphi(n)) = K_{\varphi(n)} \ (n \geq 0) \ .$$

هرگاه $\varphi(n)$ را با G_n نشان‌دهیم ،آنگاه دنباله‌ای از زیرگروههای $G_0, G_1, G_2, \ldots$ از G (که همه در S اند) را خواهیم داشت به‌طوری که

$$G = G_0;\ G_1 = K_{G_0};\ G_2 = K_{G_1}; \ldots;\ G_{n+1} = K_{G_n}; \ldots$$

بنابر ساخت ، هر G_i در G نرمال است و

$$G \gtrneqq G_1 \gtrneqq G_2 \gtrneqq G_3 \gtrneqq \cdots .$$

اگر G در شرط زنجیرکاهشی بر زیرگروههای نرمال صدق کند ، این یک تناقض می‌باشد . به علاوه ، استدلالی استقرایی نشان می‌دهد که به‌ازای هر $n \geq 1$ ، $G = G_n \times J_{G_{n-1}} \times J_{G_{n-2}} \times \cdots \times J_{G_0}$ که در آن هر J_{G_i} زیرگروهی حقیقی از G است . درنتیجه ، یک زنجیر افزایشی حقیقی از زیرگروههای نرمال وجود دارد :

$$J_{G_0} \lneqq J_{G_1} \times J_{G_0} \lneqq J_{G_2} \times J_{G_1} \times J_{G_0} \lneqq \cdots .$$

اگر G در شرط زنجیر افزایشی بر زیرگروههای نرمال صدق کند ، این یک تناقض خواهد بود .

برای‌تعیین شرایطی که تحت آنها تجزیهٔ قضیهٔ ۳۰۳ منحصر به فرد باشد ، به‌چند تعریف و لم نیاز خواهیم داشت.درونریختی f از گروه G ***درونریختی نرمال*** نامیده می‌شود اگر به‌ازای هر $a, b \in G$ ، $af(b)a^{-1} = f(aba^{-1})$.

لم ۴۰۳ . *فرض‌کنیم گروه G در شرط زنجیر افزایشی [کاهشی] بر زیرگروههای نرمال صدق کرده و f یک درونریختی [نرمال] G باشد . در این صورت ، f یک خودریختی است اگر و فقط اگر f یک برووریختی [تکریختی] باشد .*

برهان. فرض کنیم G در ACC صدق کرده و f بروریختی باشد. زنجیر افزایشی $\langle e\rangle < \operatorname{Ker} f < \operatorname{Ker} f^2 < \cdots$ (که در آن $f^k = ff\cdots f$) از زیرگروههای نرمال باید ثابت باشد؛ مثلاً $\operatorname{Ker} f^n = \operatorname{Ker} f^{n+1}$، چون f بروریختی است، f^n نیز چنین است. هرگاه $a \in G$ و $f(a) = e$، آنگاه به‌ازای $b \in G$ ای، $a = f^n(b)$ و $e = f(a) = f^{n+1}(b)$. درنتیجه، $b \in \operatorname{Ker} f^{n+1} = \operatorname{Ker} f^n$، که ایجاب می‌کند $a = f^n(b) = e$. لذا، f تکریختی و درنتیجه خودریختی است.

فرض کنیم G در DCC صدق کرده و f تکریختی باشد. به‌ازای هر $k \geq 1$، $\operatorname{Im} f^k$ در G نرمال است، زیرا f یک درونریختی نرمال می‌باشد. درنتیجه، زنجیر کاهشی $G > \operatorname{Im} f > \operatorname{Im} f^2 > \cdots$ باید ثابت باشد؛ مثلاً $\operatorname{Im} f^n = \operatorname{Im} f^{n+1}$. لذا، به‌ازای هر $a \in G$، $b \in G$ ای هست که $f^n(a) = f^{n+1}(b)$. چون f تکریختی است، f^n نیز چنین است؛ و درنتیجه، $f^n(a) = f^{n+1}(b) = f^n(f(b))$ ایجاب می‌کند که $a = f(b)$. بنابراین، f بروریختی است؛ و درنتیجه، خودریختی می‌باشد.

لم ۵.۳. (فیتینگ[1]) هرگاه گروه G در هر دو شرط زنجیر افزایشی و کاهشی بر زیرگروههای نرمال صدق کند و f یک درونریختی نرمال G باشد، آنگاه، به‌ازای $n \geq 1$ ی، $G = \operatorname{Ker} f^n \times \operatorname{Im} f^n$.

برهان. چون f یک درونریختی نرمال است، هر $\operatorname{Im} f^k$ $(k \geq 1)$ در G نرمال است. از اینرو، دو زنجیر از زیرگروههای نرمال خواهیم داشت:

$$\langle e\rangle < \operatorname{Ker} f < \operatorname{Ker} f^2 < \cdots \quad \text{و} \quad G > \operatorname{Im} f > \operatorname{Im} f^2 > \cdots$$

طبق فرض، n ی هست به‌طوری که به‌ازای هر $k \geq n$، $\operatorname{Im} f^k = \operatorname{Im} f^n$ و $\operatorname{Ker} f^k = \operatorname{Ker} f^n$. فرض کنیم $a \in \operatorname{Ker} f^n \cap \operatorname{Im} f^n$. پس به‌ازای $b \in G$ ای، $a = f^n(b)$ و $f^{2n}(b) = f^n(f^n(b)) = f^n(a) = e$. درنتیجه، $b \in \operatorname{Ker} f^{2n} = \operatorname{Ker} f^n$، پس $a = f^n(b) = e$. بنابراین، $\operatorname{Ker} f^n \cap \operatorname{Im} f^n = \langle e\rangle$. به‌ازای هر $c \in G$، $f^n(c) \in \operatorname{Im} f^n = \operatorname{Im} f^{2n}$، که از آنجا به‌ازای $d \in G$ ای، $f^n(c) = f^{2n}(d)$. لذا،

$$f^n(cf^n(d^{-1})) = f^n(c) f^{2n}(d^{-1}) = f^n(c) f^{2n}(d)^{-1} = f^n(c) f^n(c)^{-1} = e$$

و درنتیجه، $cf^n(d^{-1}) \in \operatorname{Ker} f^n$. چون $c = (cf^n(d^{-1})) f^n(d)$، نتیجه می‌گیریم که $G = (\operatorname{Ker} f^n)(\operatorname{Im} f^n)$. بنابراین، طبق تعریف I . ۸.۸، $G = \operatorname{Ker} f^n \times \operatorname{Im} f^n$.

1. Fitting

درونریختی f از گروه G را **پوچ توان** گوییم اگر عدد صحیح مثبتی مانند n باشد به‌طوری که به‌ازای هر $g \in G$ ، $f^n(g) = e$.

نتیجهٔ ۶.۳ . هرگاه G یک گروه تجزیه‌ناپذیر باشد که در شرایط زنجیرافزایشی و کاهشی برزیرگروههای نرمال صدق کند و f یک درونریختی نرمال G باشد ، آنگاه f یا پوچ‌توان است یا خودریختی .

برهان . به‌ازای $n \geq 1$ ی ، طبق لم فیتینگ ، داریم $G = \operatorname{Ker} f^n \times \operatorname{Im} f^n$. چون G تجزیه‌ناپذیر است ، $\operatorname{Ker} f^n = \langle e \rangle$ یا $\operatorname{Im} f^n = \langle e \rangle$. شق دوم ایجاب می‌کند که f پوچ‌توان باشد . هرگاه $\operatorname{Ker} f^n = \langle e \rangle$ ، آنگاه $\operatorname{Ker} f = \langle e \rangle$ و f تکریختی است . بنابراین ، طبق لم ۴.۳ ، f خودریختی می‌باشد .

اگر f و g درونریختیهایی از گروه G باشند ، $f+g$ **تابعی** است مانند $G \to G$ که با $a \mapsto f(a)g(a)$ داده می‌شود . در حالت کلی ، $f+g$ درونریختی **نیست** (تمرین ۷) . امابه‌آسانی دیده می‌شود که $+$ شرکتپذیر است ؛ درنتیجه ، مجموعهٔ تمام درونریختیهای G تحت $+$ یک تکگون می‌باشد (با درونریختی همانی $0_G : G \to G$ که به‌ازای هر $a \in G$ با $a \mapsto e$ داده می‌شود) .

نتیجهٔ ۷.۳ . فرض کنیم G ($\neq \langle e \rangle$) یک گروه تجزیه‌ناپذیر باشد که در هر دو شرط زنجیرافزایشی و کاهشی برزیرگروههای نرمال صدق می‌کند . هرگاه $f_1, \ldots, f_n$ درونریختیهای پوچ‌توان نرمالی از G باشند به‌طوری که هر $f_{i_1} + \cdots + f_{i_r}$ $(1 \leq i_1 < i_2 < \cdots < i_r \leq n)$ درونریختی باشد ، آنگاه $f_1 + f_2 + \cdots + f_n$ پوچ‌توان است .

طرح برهان . چون هر $f_{i_1} + \cdots + f_{i_r}$ درونریختی نرمال است (تمرین ۸ (پ)) ، مطلب به‌محض ثابت شدن حالت $n = 2$ به استقرا نتیجه می‌شود . اگر $f_1 + f_2$ پوچ‌توان نباشد ، طبق نتیجهٔ ۶.۳ یک خودریختی است . تحقیق کنیدکه معکوس g از $f_1 + f_2$ یک خودریختی نرمال است . هرگاه $g_1 = f_1 g$ و $g_2 = f_2 g$ ، آنگاه $1_G = g_1 + g_2$ و به‌ازای هر $x \in G$ ،
$x^{-1} = (g_1 + g_2)(x^{-1}) = g_1(x^{-1})g_2(x^{-1})$. از اینرو ،

$$x = [g_1(x^{-1})g_2(x^{-1})]^{-1} = g_2(x)g_1(x) = (g_2 + g_1)(x)$$

و $g_1 + g_2 = g_2 + g_1$ ، بنابراین $1_G = g_2 + g_1$.

$$g_1(g_1 + g_2) = g_1 1_G = 1_G g_1 = (g_1 + g_2)g_1,$$

که ایجاب می‌کند که $g_1 g_2 = g_2 g_1$. حال استدلال استقرایی جداگانه‌ای نشان می‌دهد که به‌ازای هر $m \geq 1$ ،

$$(g_1 + g_2)^m = \sum_{i=0}^{m} c_i g_1^i g_2^{m-i} \quad (c_i \in \mathbf{Z}),$$

که در آن c_i ها ضرایب دوجمله‌ای‌اند (ر.ک. قضیهٔ III ۶۰۱) و $c_i h$ یعنی $h + h + \cdots + h$ (c_i جمعوند). چون هر f_i پوچتوان است، $g_i = f_i g$ هسته‌ای نابدیهی دارد، که از آنجا، طبق نتیجهٔ ۶۰۳، g_i پوچتوان است. بنابراین، به‌ازای m به‌قدر کافی بزرگ و هر $a \in G$ ،

$$(g_1 + g_2)^m(a) = \sum_{i=0}^{m} c_i g_1^i g_2^{m-i}(a) = \prod_{i=0}^{m} e^{c_i} = e.$$

اما این با $g_1 + g_2 = 1_G$ و $G \neq \langle e \rangle$ متناقض می‌باشد.

در قضیهٔ بعدی از نکات زیر استفاده خواهیم کرد. هرگاه گروه G حاصلضرب مستقیم داخلی زیرگروههای $G_1, \ldots, G_s$ خودباشد، آنگاه، بنابربرهان قضیهٔ I ۶۰۸، یک یکریختی مانند $\varphi : G_1 \times \cdots \times G_s \cong G$ وجود دارد که با $(g_1, \ldots, g_s) \mapsto g_1 g_2 \cdots g_s$ داده می‌شود. درنتیجه، هر عنصر G را می‌توان به‌طورمنحصربه‌فرد به صورت حاصلضربی چون $g_1 g_2 \cdots g_s$ $(g_i \in G_i)$ نوشت. به‌ازای هر i ، نگاشت $\pi_i : G \to G_i$ داده شده با $g_1 g_2 \cdots g_s \mapsto g_i$ یک برووریختی تعریف شده است (این نگاشت ترکیب φ^{-1} با تصویر کانونی $G_1 \times \cdots \times G_s \to G_i$ می‌باشد.) نگاشتهای π_i را برووریختیهای کانونی وابسته به حاصلضرب مستقیم داخلی $G = G_1 \times \cdots \times G_s$ می‌نامیم.

قضیهٔ ۸۰۳ (کرول ــ اشمیت). *فرض کنیم گروه G در هر دو شرط زنجیر افزایشی و کاهشی برزیرگروههای نرمال صدق کند. هرگاه $G = G_1 \times G_2 \times \cdots \times G_s$ و $G = H_1 \times H_2 \times \cdots \times H_t$ و هر G_i, H_j تجزیه‌ناپذیر باشند، آنگاه $s = t$ و، پس از اندیسگذاری مجدد، به‌ازای هر i ، $G_i \cong H_i$ ، و به‌ازای هر $r < t$ ،*

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t.$$

چند تبصره. بنابرقضیهٔ ۳.۳ ، G دست کم یک چنین تجزیه‌ای را دارد . حکم یکتایی در اینجا قویتر از آن است که صرفا " بگوییم عاملهای تجزیه‌ناپذیر با تقریب یکریختی معین شده‌اند .

طرح برهان ۸.۳ . فرض کنیم $P(0)$ عبارت $G = H_1 \times \cdots \times H_t$ باشد . به‌ازای $1 \leq r \leq \min(s,t)$ ، فرض کنیم $P(r)$ حکم زیر باشد : تغییر اندیسی از $H_1, \ldots, H_t$ وجود دارد به‌طوری که به‌ازای $i = 1,2, \ldots, r$ ، $G_i \cong H_i$ و $G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t$ (یا $G = G_1 \times \cdots \times G_t$ اگر $r = t$) . به‌استقرا نشان می‌دهیم که $P(r)$ به‌ازای هر r که $0 \leq r \leq \min(s,t)$ درست‌است . $P(0)$ طبق فرض درست است ؛ و درنتیجه ، فرض می‌کنیم $P(r-1)$ درست باشد ؛ پس از اندیسگذاری مجدد ، به‌ازای $i = 1, \ldots, r-1$ ، $G_i \cong H_i$ و $G = G_1 \times \cdots \times G_{r-1} \times H_r \times \cdots \times H_t$. فرض کنیم بروریختیهای کانونی $\pi_1, \ldots, \pi_s$ [$\pi_1', \ldots, \pi_t'$] وابسته به حاصلضرب مستقیم داخلی

$$G = G_1 \times \cdots \times G_s \; [\, G = G_1 \times \cdots \times G_{r-1} \times H_r \times \cdots \times H_t]$$

همانند بند پیش از صورت قضیه باشد . همچنین ، λ_i [λ_i'] نگاشتهای شمول باشند که عامل i ام را به توی G می‌برند . به‌ازای هر i ، فرض کنیم $\varphi_i = \lambda_i\pi_i : G \to G$ و $\psi_i = \lambda_i'\pi_i' : G \to G$. تحقیق کنید که اتحادهای زیر برقرارند :

$\varphi_i \mid G_i = 1_{G_i}$;	$\varphi_i\varphi_i = \varphi_i$;	$\varphi_i\varphi_j = 0_G \; (i \neq j)$[1];
$\psi_1 + \cdots + \psi_t = 1_G$;	$\psi_i\psi_i = \psi_i$;	$\psi_i\psi_j = 0_G \; (i \neq j)$;
$\operatorname{Im} \varphi_i = G_i$;	$\operatorname{Im} \psi_i = G_i \; (i < r)$;	$\operatorname{Im} \psi_i = H_i \; (i \geq r)$.

از اینجا نتیجه می‌شود که به‌ازای هر $i < r$ ، $\varphi_r\psi_i = 0_G$ (زیرا $\psi_i(x) \in G_i$) ؛ درنتیجه ، $\varphi_r\psi_i(x) = \varphi_r 1_G \psi_i(x) = \varphi_r\varphi_i\psi_i(x) = e$.

اتحادهای فوق نشان می‌دهند که

$$\varphi_r = \varphi_r 1_G = \varphi_r(\psi_1 + \cdots + \psi_t) = \varphi_r\psi_r + \cdots + \varphi_r\psi_t.$$

---

۱ . ر.ک. بند پیش از نتیجهٔ ۷.۳ .

هر "مجموع" از $\varphi_r\psi_i$ یک درونریختی نرمال است (تمرینهای ۸ و ۹) . چون $\varphi_r \mid G_r = 1_{G_r}$ یک خودریختی (نرمال) از G_r است و G_r در هر دو شرط زنجیری بر زیرگروههای نرمال صدق می‌کند (تمرین ۶) ، نتایج ۶.۳ و ۷.۳ ایجاب می‌کنند که $\varphi_r\psi_i \mid G_r$ یک خودریختی از G_r به‌ازای $r \le j \le t$ ای $G_r \neq \langle e \rangle$ باشد . بنابراین ، به‌ازای هر $n \ge 1$ ، $(\varphi_r\psi_j)^{n+1}$ نیز یک خودریختی از G می‌باشد . درنتیجه ، چون $G_r \neq \langle e \rangle$ و به‌ازای هر $n \ge 1$ ، $(\varphi_r\psi_j)^{n+1} = \varphi_r(\psi_j\varphi_r)^n\psi_j$ ، درونریختی نرمال $\psi_j\varphi_r \mid H_j : H_j \to H_j$ نمی‌تواند پوچ‌توان باشد . چون H_j درهردوشرط زنجیری صدق می‌کند (تمرین ۶) ، بنابر نتیجهٔ ۷.۳ ، $\psi_j\varphi_r \mid H_j$ باید یک خودریختی از H_j باشد . بنابراین ، $\psi_j \mid G_r : G_r \to H_j$ یک یکریختی است ؛ و درنتیجه ، $\varphi_r \mid H_j : H_j \to G_r$ نیز چنین است . H_k ها را طوری تغییر اندیس می‌دهیم که بتوان فرض کرد $j = r$ و $G_r \cong H_r$. پس نیمهٔ اول حکم $P(r)$ را ثابت کرده‌ایم .

چون $G = G_1 \times \cdots \times G_{r-1} \times H_r \times \cdots \times H_t$ ، طبق فرض استقرا ، زیرگروه $G_1 \times \cdots G_{r-1} \times H_{r+1} \times \cdots \times H_t$ حاصلضرب مستقیم داخلی $G_1G_2 \cdots G_{r-1}H_{r+1} \cdots H_t$ است . توجه کنید که به‌ازای $j < r$ ، $\psi_r(G_j) = \psi_r\psi_j(G) = \langle e \rangle$ و به‌ازای $j > r$ ، $\psi_r(H_j) = \psi_r\psi_j(G) = \langle e \rangle$ ، که از آنجا $\psi_r(G_1 \cdots G_{r-1}H_{r+1} \cdots H_t) = \langle e \rangle$. چون $\psi_r \mid G_r$ یکریختی است ، باید داشته باشیم

$$G_r \cap (G_1 \cdots G_{r-1}H_{r+1} \cdots H_t) = \langle e \rangle .$$

پس نتیجه می‌شود که گروه $G^* = G_1 \cdots G_{r-1}G_rH_{r+1} \cdots H_t$ حاصلضرب مستقیم داخلی زیر است :

$$G^* = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t.$$

نگاشت $\theta : G \to G$ را به‌صورت زیر تعریف می‌کنیم . هر عنصر $g \in G$ را می‌توان به صورت $g = g_1 \cdots g_{r-1}h_r \cdots h_t$ نوشت که $g_i \in G_i$ و $h_i \in H_i$. فرض کنیم

$$\theta(g) = g_1 \cdots g_{r-1}\varphi_r(h_r)h_{r+1} \cdots h_t.$$

واضح است که $\operatorname{Im}\theta = G^*$. θ یک‌تکریختی است (ر.ک. قضیهٔ ۱۰.۸.۱) که به‌آسانی معلوم می‌شود که نرمال است . لذا ، طبق لم ۴.۳ ، θ یک خودریختی است ؛ درنتیجه ، $G = \operatorname{Im}\theta = G^* = G_1 \times \cdots G_r \times H_{r+1} \times \cdots \times H_t$. این قسمت دوم $P(r)$ را ثابت و استقرا را کامل می‌کند . لذا ، پس از اندیسگذاری مجدد ، به‌ازای $0 \le i \le \min(s,t)$ ، هرگاه $G_i \cong H_i$. آنگاه $\min(s,t) = s$ ،

$$G_1 \times \cdots \times G_s = G = G_1 \times \cdots \times G_s \times H_{s+1} \times \cdots \times H_t,$$

و هرگاه $\min(s,t) = t$ ، آنگاه $G_1 \times \cdots \times G_s = G = G_1 \times \cdots \times G_t$ ، چون به‌ازای هر i,j ، $G_i \neq \langle e \rangle$, $H_i \neq \langle e \rangle$ ، باید درهر حال داشته باشیم $s = t$.

تمرینات

۱ . گروه G تجزیه‌ناپذیر است اگر و فقط اگر $G \neq \langle e \rangle$ و $G \cong H \times K$ ایجاب کنند که $H = \langle e \rangle$ یا $K = \langle e \rangle$.

۲ . S_n به‌ازای هر $n \geq 2$ تجزیه‌ناپذیر است . [**راهنمایی .** اگر $n \geq 5$ ، قضایای I . ۸۰۶ و I . ۱۰۰۶ و تمرین I . ۷۰۸ ممکن است مفید واقع شوند .]

۳ . گروه جمعی $\mathbf{Q}$ تجزیه‌ناپذیر است .

۴ . نقش همریخت نابدیهی یک گروه تجزیه ناپذیر لزوما " تجزیه‌ناپذیر نیست .

۵ . (آ) $\mathbf{Z}$ در ACC بر زیرگروهها صدق می‌کند ولی در DCC صدق نمی‌کند .
(ب) هر گروه آبلی با تولید متناهی در ACC بر زیرگروهها صدق می‌نماید .

۶ . فرض کنید H,K زیرگروههای نرمال گروه G باشند به‌طوری که $G = H \times K$.
(آ) هرگاه N زیرگروه نرمالی از H باشد ، آنگاه N در G نرمال است (با تمرین I . ۱۰۰۵ مقایسه کنید) .
(ب) هرگاه G در ACC یا DCC بر زیرگروههای نرمال صدق کند ، H و K نیز چنین خواهند کرد .

۷ . هرگاه f و g درونریختیهایی از گروه G باشند ، آنگاه $f+g$ لزوما " درونریختی نیست . [**راهنمایی .** فرض کنید $a = (123)$, $b = (132) \in S_3$ و تعریف کنید $f(x) = axa^{-1}$, $g(x) = bxb^{-1}$.]

۸ . فرض کنید f و g درونریختیهای نرمالی از گروه G باشند .
(آ) fg یک درونریختی نرمال است .
(ب) $H \lhd G$ ایجاب می‌کند که $f(H) \lhd G$.
(پ) هرگاه $f+g$ یک درونریختی باشد ، آنگاه نرمال است .

۹ . فرض کنید $G = G_1 \times \cdots \times G_n$. به‌ازای هر i ، $\lambda_i : G_i \to G$ را نگاشت شمول و $\pi_i : G \to G_i$ را تصویرکانونی بگیرید (ر . ک . صفحهٔ ۹۱) . فرض کنید $\varphi_i = \lambda_i \pi_i$. در این صورت ، "مجموع" $\varphi_{i_1} + \cdots + \varphi_{i_k}$ هر k تا $(1 \leq k \leq n)$ φ_i **متمایز** یک درونریختی از G است .

۱۰ . با استفاده‌ازقضیهٔ کرول ـ اشمیت ، قضایای ۲.۲ و ۶.۲ (سه) برای گروههای آبلی متناهی را ثابت کنید .

۱۱ . هرگاه G و H گروههایی باشند به‌طوری‌که $G \times G \cong H \times H$ و G در ACC و DCC برزیرگروههای نرمال صدق کند ، آنگاه $G \cong H$ [ر.ک. تمرین ۱۱.۲] .

۱۲ . هرگاه G ، K ، H ، و J گروههایی باشند به‌طوری‌که $G \cong H \times K$ و $G \cong H \times J$ و G در ACC و DCC برزیرگروههای نرمال صدق کند ، آنگاه $K \cong J$ [ر.ک. تمرین ۱۱.۲] .

۱۳ . به‌ازای هر p اول ، گروه $Z(p^\infty)$ در شرط زنجیر کاهشی بر زیرگروهها صدق می‌کند ولی در شرط افزایشی صدق نمی‌کند . [ر.ک. تمرین I، ۳. ۷].

۴ عمل یک گروه بر یک مجموعه

تکنیکهای این بخش را در بخشهای آتی برای عرضهٔ قضایای ساختاری درمورد گروههای (غیرآبلی متناهی) به کار خواهیم برد .

تعریف ۱.۴ . گوییم گروه G **بر مجموعهٔ** S **عمل می‌کند** اگر تابعی مانند $G \times S \to S$ (که معمولا " با $(g,x) \mapsto gx$ نموده‌می‌شود)وجود داشته باشد به‌طوری که به‌ازای هر $x \in S$ و $g_1, g_2 \in G$ ،

$$ex = x \quad \text{و} \quad (g_1g_2)x = g_1(g_2x) .$$

چون ممکن است گروه G به طرق مختلف بر S عمل کند ، نماد gx مبهم است . اما این مشکلی ایجاد نخواهد کرد .

مثال . یک عمل‌گروه متقارن S_n بر مجموعهٔ $I_n = \{1,2,\ldots,n\}$ به صورت $(\sigma,x) \to \sigma(x)$ داده می‌شود .

چند مثال . فرض کنیم G یک‌گروه و H زیرگروهی از آن باشد . یک عمل گروه H بر مجموعهٔ G با $(h,x) \mapsto hx$ داده می‌شود ، که در آن hx حاصلضرب در G است . عمل $h \in H$ بر G یک **انتقال** (چپ) نام دارد . هرگاه K زیرگروه دیگری از G و S مجموعهٔ

تمام هم‌مجموعه‌های K در G باشد، آنگاه H بر S به وسیلهٔ انتقال $(h,xK)\mapsto hxK$ عمل می‌کند.

چند مثال. فرض کنیم H زیرگروهی از گروه G باشد. یک عمل H بر مجموعهٔ G با $(h,x)\mapsto hxh^{-1}$ داده می‌شود؛ برای آنکه با ضرب در G اشتباه نشود، این عمل $h\in H$ همواره با hxh^{-1} نموده می‌شود **نه** با hx. این عمل $h\in H$ بر G **تزویج** به‌وسیلهٔ h نام دارد و گوییم عنصر hxh^{-1} **مزدوج** x است. هرگاه K زیرگروهی از G بوده و $h\in H$، آنگاه hKh^{-1} زیرگروهی از G است که با K یکریخت می‌باشد (تمرین ۱ . ۶۰۵). ازاینرو، H بر مجموعهٔ S جمیع زیرگروههای G به‌وسیلهٔ تزویج $(h,K)\mapsto hKh^{-1}$ عمل می‌کند. گوییم گروه hKh^{-1} **مزدوج** K می‌باشد.

قضیهٔ ۲۰۴. **فرض کنیم گروه G بر مجموعهٔ S عمل کند.**

(یک) رابطهٔ تعریف شده با

$$x\sim x' \leftrightarrow gx = x' \text{ ، به‌ازای } g\in G \text{ ای}$$

بر S یک رابطهٔ هم‌ارزی است.

(دو) به‌ازای هر $x\in S$، $G_x = \{g\in G \mid gx = x\}$ زیرگروهی از G است.

برهان. تمرین.

رده‌های هم‌ارزی رابطهٔ هم‌ارزی قضیهٔ ۲۰۴ (یک) **مدارهای**[1] G بر S نام دارند؛ مدار $x\in S$ با $\bar{x}$ نموده می‌شود. زیرگروه G_x گاهی **زیرگروه ثابت ساز** x، گروه یکسویی x، یا **پایدارساز** x خوانده می‌شود.

چند مثال. هرگاه گروه G به‌وسیلهٔ تزویج برخودش عمل کند، آنگاه مدار $\{gxg^{-1} \mid g\in G\}$ عنصر $x\in G$ **ردهٔ ازدواج** x نامیده می‌شود. اگر زیرگروه H بر G به وسیلهٔ تزویج عمل

---

۱. *این با استفادهٔ قبلی ما از واژهٔ مدار در برهان قضیهٔ ۱ . ۳۰۶، که در آن حالت خاص یک زیرگروه دوری $\langle\sigma\rangle$ از S_n بر مجموعهٔ I_n عمل می‌کرد، سازگار است.*

کند ، گروه یکسویی

$$H_x = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\}$$

را مرکزساز x در H نامندوبا $C_H(x)$ نشان می‌دهند . اگر $H = G$ ، $C_G(x)$ فقط مرکزساز x نامیده می‌شود . هرگاه H به وسیلهٔ تزویج بر مجموعهٔ S جمیع زیرگروههای G عمل کند ،آنگاه‌زیرگروهی‌از H که‌ثابت‌ساز $K \in S$ است ،یعنی $\{h \in H \mid hKh^{-1} = K\}$ ، نرمال‌ساز K در H نام دارد و با $N_H(K)$ نموده‌می‌شود .گروه $N_G(K)$ را فقط نرمال‌ساز K می‌نامیم . واضح است که هر زیرگروه K در $N_G(K)$ نرمال است ؛ K در G نرمال است اگر و فقط اگر $N_G(K) = G$.

قضیهٔ ۳۰۴ . هرگاه گروه G بر مجموعهٔ S عمل کند ، آنگاه عدد اصلی مدار $x \in S$ اندیس $[G : G_x]$ است .

برهان . فرض کنیم $g,h \in G$. چون

$$gx = hx \Leftrightarrow g^{-1}hx = x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow hG_x = gG_x,$$

نتیجه می‌شود کـه نگاشت داده شده با $gG_x \mapsto gx$ یک بیژکسیون تعریف شده از مجموعهٔ هم‌مجموعه‌های G_x در G به‌روی‌مدار $\bar{x} = \{gx \mid g \in G\}$ است . بنابراین ، $[G : G_x] = |\bar{x}|$.

نتیجهٔ ۴۰۴ . فرض‌کنیم G گروهی متناهی و K زیرگروهی از G باشد .

(یک) تعداد عناصر در ردهٔ ازدواج $x \in G$ مساوی $[G : C_G(x)]$ است ،که $|G|$ را عاد می‌کند ؛

(دو) هرگاه $\bar{x}_1, \ldots, \bar{x}_n$ $(x_i \in G)$ رده‌های ازدواج متمایزی از G باشند ، آنگاه

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)];$$

(سه) تعدادزیرگروههای G مزدوج‌با K مساوی $[G : N_G(K)]$ است ،که $|G|$ را عادمی‌کند .

برهان . (یک)و (سه) بی‌درنگ ازقضیهٔ‌قبل‌و قضیهٔ لاگرانژ I . ۶.۴ نتیجه می‌شوند . چون ازدواج یـک رابطهٔ هم‌ارزی بر G است (قضیهٔ ۲.۴) ، G احتماع ازهم‌جدایی از رده‌های ازدواج $\bar{x}_1, \ldots, \bar{x}_n$ است ؛ درنتیجه ، (دو) از (یک) نتیجه می‌شود .

معادلهٔ $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$ را، همانند در نتیجهٔ ۴.۴ (دو)، **معادلهٔ ردهای** گروه متناهی G می‌نامند.

قضیهٔ ۵.۴. **هرگاه گروه G بر مجموعهٔ S عمل کند، آنگاه این عمل یک همریختی مانند $G \to A(S)$ القا می‌کند، که در آن $A(S)$ گروه تمام جایگشتهای S است.**

برهان. اگر $g \in G$ ، $\tau_g : S \to S$ را با $x \mapsto gx$ تعریف می‌کنیم. چون به‌ازای هر $x \in S$ ، $x = g(g^{-1}x)$ ، τ_g سورژکتیو است. به همین نحو، $gx = gy$ $(x,y \in S)$ ایجاب می‌کند که $x = g^{-1}(gx) = g^{-1}(gy) = y$ ؛ درنتیجه، τ_g انژکتیو و لذا بیژکسیون (جایگشت S) می‌باشد. چون به‌ازای هر $g,g' \in G$ ، $\tau_{gg'} = \tau_g\tau_{g'} : S \to S$ ، نگاشت $G \to A(S)$ داده‌شده با $g \mapsto \tau_g$ یک همریختی است.

نتیجهٔ ۶.۴ (کیلی[1]). **هرگاه G گروه باشد، آنگاه یک تکریختی مانند $G \to A(G)$ وجود دارد. از اینرو، هر گروه با یک گروه از جایگشتها یکریخت است. بخصوص، هرگروه متناهی با زیرگروهی از S_n ، که $n = |G|$ ، یکریخت است.**

برهان. فرض کنیم G به وسیلهٔ انتقال چپ بر خودش عمل کند و، با اعمال قضیهٔ ۵.۴ ، یک همریختی مانند $\tau : G \to A(G)$ به دست می‌آوریم. هرگاه $\tau(g) = \tau_g = 1_G$ ، آنگاه به‌ازای هر $x \in G$ ، $gx = \tau_g(x) = x$. بخصوص، $ge = e$ ؛ درنتیجه، $g = e$ و τ یک تکریختی است. برای اثبات آخرین حکم، توجه می‌کنیم که هرگاه $|G| = n$ ، آنگاه $A(G) \cong S_n$.

به یاد آورید که هرگاه G گروه باشد، آنگاه مجموعهٔ $\mathrm{Aut}\, G$ مرکب از تمام خودریختیهای G باترکیب توابع به‌عنوان عملی دوتایی یک گروه است (تمرین I ۱۵۰۲۰).

---

1. *Cayley*

نتیجهٔ ۷.۴ . *فرض کنیم* G *یک گروه باشد .*

(یک) به‌ازای هر $g \in G$ *، تزویج به وسیلهٔ* g *یک خودریختی از* G *را القا می‌کند .*

(دو) یک همریختی مانند $G \to Aut\ G$ *وجود دارد که هسته‌اش مساوی است با*

$$\{g \in G \mid gx = xg \text{ ، به‌ازای هر } x \in G\}$$

برهان . (یک) هرگاه G به‌وسیلهٔ تزویج بر خودش عمل کند ، آنگاه به‌ازای هر $g \in G$ ، نگاشت $\tau_g : G \to G$ داده شده با $\tau_g(x) = gxg^{-1}$ ، طبق برهان قضیهٔ ۵.۴ ، یک بیژکسیون است . به‌آسانی معلوم می‌شود که τ_g یک همریختی نیز هست ؛ و درنتیجه ، یک خودریختی است . (دو) فرض کنیم G به وسیلهٔ تزویج برخودش عمل کند . بنابر (یک) ، نقش همریختی $\tau : G \to A(G)$ قضیهٔ ۵.۴ مشمول Aut G است . واضح است که

به‌ازای هر $x \in G$ ، $g \in \text{Ker } \tau \Leftrightarrow \tau_g = 1_G \Leftrightarrow gxg^{-1} = \tau_g(x) = x$.

اما $gxg^{-1} = x$ اگر و فقط اگر $gx = xg$ ، که از آنجا $\text{Ker } \tau = C(G)$.

خودریختی τ_g نتیجهٔ ۷.۴ (یک) **خودریختی داخلی** القا شده به وسیلهٔ g نام دارد . زیرگروه نرمال $C(G) = \text{Ker } \tau$ **مرکز** G نامیده می‌شود . عنصر $g \in G$ در $C(G)$ است اگر و فقط اگر ردهٔ ازدواج g فقط از g تشکیل شده باشد . لذا ، هرگاه G متناهی بوده و $x \in C(G)$ ، آنگاه $[G : C_G(x)] = 1$ (نتیجهٔ ۴.۴) . درنتیجه ، معادلهٔ رده‌ای G (نتیجهٔ ۴.۴ (دو)) را می‌توان به صورت زیر نوشت :

$$|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)],$$

که در آن $x_1, \ldots, x_m$ $(x_i \in G - C(G))$ رده‌های ازدواج متمایز G بوده و هر $[G : C_G(x_i)] > 1$.

حکم ۸.۴ . *فرض کنیم* H *زیرگروهی از گروه* G *بوده و* G *به وسیلهٔ انتقال چپ بر مجموعهٔ* S *مرکب از جمیع هم‌مجموعه‌های چپ* H *در* G *عمل نماید . در این صورت ، هستهٔ همریختی القا شدهٔ* $G \to A(S)$ *مشمول* H *می‌باشد .*

برهان . همریختی القا شدهٔ $G \to A(S)$ با $g \mapsto \tau_g$ داده می‌شود ، که در آن $\tau_g : S \to S$

و $\tau_g(xH) = gxH$. هرگاه g در هسته باشد، آنگاه $\tau_g = 1_S$ و، به‌ازای هر $x \in G$ ، $gxH = xH$ ؛ بخصوص، به‌ازای $x = e$ ، $geH = eH = H$ ، که‌ایجاب می‌کندکه $g \in H$.

نتیجهٔ ۹۰۴ . هرگاه H زیرگروهی با اندیس n در گروه G بوده و هیچ زیرگروه نرمال نابدیهی G مشمول H نباشد، آنگاه G با زیرگروهی از S_n یکریخت است.

برهان. حکم ۸۰۴ را بر H اعمال می‌کنیم ؛ هستهٔ $G \to A(S)$ زیرگروه نرمالی از G مشمول H است و لذا، طبق فرض، باید مساوی $\langle e \rangle$ باشد. از اینرو، $G \to A(S)$ یک تکریختی است. لذا، G با زیرگروهی ازگروه تمام جایگشتهای n هم مجموعهٔ چپ H یکریخت است، و گروه اخیر بوضوح با S_n یکریخت می‌باشد.

نتیجهٔ ۱۰۴ . هرگاه H زیرگروهی از گروه متناهی G با اندیس p باشد، که p کوچکترین عدد اولی است که مرتبهٔ G را عاد می‌کند، آنگاه H در G نرمال است.

برهان. فرض کنیم S مجموعهٔ تمام هم‌مجموعه‌های چپ H در G باشد. در این صورت، $A(S) \cong S_p$ ، زیرا $[G : H] = p$. هرگاه K هستهٔ همریختی $G \to A(S)$ حکم ۸۰۴ باشد، آنگاه K در G نرمال‌بوده‌و مشمول H است. به‌علاوه، G/K با زیرگروهی از S_p یکریخت است. از اینرو، $|G/K|$ ، $|S_p| = p$ را عاد می‌کند. اما هر مقسوم‌علیه $|G/K| = [G : K]$ باید $|G| = |K|\,[G : K]$ را عاد کند. چون هیچ عدد کوچکتر از p (جز 1) نمی‌تواند $|G|$ را عاد کند، باید داشته باشیم $|G/K| = 1$ یا p . اما

$$|G/K| = [G : K] = [G : H][H : K] = p[H : K] \geq p .$$

بنابراین، $|G/K| = p$ و $[H : K] = 1$ ؛ درنتیجه، $H = K$. اما K در G نرمال است.

تمرینات

۱ . فرض کنید G گروه و A زیرگروه آبلی نرمالی از آن باشد. نشان دهید G/A به وسیلهٔ تزویج بر A عمل می‌کند و یک همریختی مانند $G/A \to \mathrm{Aut}\, A$ به دست آورید.

۲ . اگر H, K زیرگروههایی از G باشندبه‌طوری‌که $H \lhd K$ ،نشان‌دهیدکه $K < N_G(H)$.

۳ . هرگاه گروه G شامل عنصری مانند a با دقیقاً " دو مزدوج باشد ، آنگاه G دارای زیرگروه نرمال حقیقی مانند $N \neq \langle e \rangle$ است .

۴ . فرض کنید H زیرگروهی از G باشد . مرکزساز H مجموعه‌ای است مانند { بهازای هر $h \in H$ ، $C_G(H) = \{g \in G \mid hg = gh\}$. نشان دهیدکه $C_G(H)$ زیرگروهی از $N_G(H)$ است .

۵ . اگر H زیرگروهی از G باشد ، گروه عاملی $N_G(H)/C_G(H)$ (ر.ک. تمرین ۴) با زیرگروهی از $\mathrm{Aut}\, H$ یکریخت است .

۶ . فرض کنید G گروهی باشدکه برمجموعهٔ S که دست‌کم دو عنصر دارد عمل می‌کند . همچنین ، G متعدی باشد ؛ یعنی ، بهازای هر $x,y \in S$ ، $g \in G$ ای وجود داشته باشد بهطوری که $gx = y$. ثابت کنید

(آ) بهازای $x \in S$ ، مدار $\bar{x}$ از x مساوی S است ؛

(ب) تمام پایدارسازهای G_x (بهازای $x \in S$) مزدوج یکدیگرند ؛

(پ) هرگاه G دارای خاصیت زیر باشد :

$$\{g \in G \mid gx = x \text{ ، بهازای هر } x \in S\} = \langle e \rangle$$

(که حالتی است که بهازای n ی ، $G < S_n$ و $S = \{1,2,\ldots,n\}$ و $N \lhd G$ و بهازای $x \in S$ ی ، $N < G_x$ ، آنگاه $N = \langle e \rangle$ ؛

(ت) بهازای $x \in S$ ی ، $|S| = [G : G_x]$ ؛ درنتیجه $|S|$ ، $|G|$ را عاد می‌کند .

۷ . فرض کنید G گروه و $\mathrm{In}\, G$ مجموعهٔ تمام خودریختیهای داخلی G باشد . نشان دهید که $\mathrm{In}\, G$ یک زیرگروه نرمال $\mathrm{Aut}\, G$ است .

۸ . یک خودریختی از Z_6 نشان دهید که خودریختی داخلی **نباشد** .

۹ . هرگاه $G/C(G)$ دوری باشد ، آنگاه G آبلی است .

۱۰ . نشان دهید که مرکز S_4 مساوی $\langle e \rangle$ است ؛ نتیجه بگیریدکه S_4 با گروه تمام خودریختیهای داخلی S_4 یکریخت است .

۱۱ . فرض کنید G گروهی باشد شامل عنصر a که مرتبه‌اش 1 یا 2 نیست . نشان دهید که G دارای یک خودریختی غیرهمانی است . [**راهنمایی** . تمرین I . ۲ . ۲۰ و نتیجهٔ ۷ . ۴ .]

۱۲ . هرگروه متناهی با زیرگروهی از A_n ، بهازای n ی ، یکریخت است .

۱۳ . اگر گروه G شامل زیرگروهی $(\neq G)$ با اندیس متناهی باشد ، حاوی زیرگروه نرمالی $(\neq G)$ با اندیس متناهی است .

۱۴ . هرگاه $|G| = pn$ ، کـه در آن $p > n$ و p اول است ، و H زیرگروهی از مرتبهٔ p باشد ، آنگاه H در G نرمال است .

۱۵ . هرگاه زیرگروه نرمال N از مرتبهٔ p (p اول) مشمول گروه G از مرتبهٔ p^n باشد ، آنگاه N در مرکز G است .

۵ قضایای زیلوف[1]

گروههای متنـاهی غیرآبلی از گروههای آبلی متناهی ، که در بخش ۲ کاملا " (با تقریب یکریختی) رده‌بندی شـدند ، بسیار پیچیده‌ترند . قضایای زیلوف اولین گام اساسی در درک ساختار یک گروه متناهی دلخواه می‌باشند .

انگیزهٔ ماسئوال‌زیراست : اگر عدد صحیـح و مثبت m مرتبهٔ گروه G را عاد کند ، آیا G زیرگروهی از مـرتبهٔ m دارد ؟ این عکس قضیهٔ لاگرانژ I . ۶.۴ است . این امر برای گروههای آبلی صحیح است (نتیجهٔ ۴.۲) ولی ممکن است برای گروههای دلخواه صحیح نباشد (تمرین I . ۸.۶۰) . ابتداحالت خاصی که m اول است را در نظر می‌گیریم (قضیهٔ ۲.۵) ، و سپس به قضیهٔ اول‌زیلوف می‌پردازیم که می‌گوید جواب سوال وقتی m توانی از یک عدد اول باشد مثبت است . این طبعا " ما را به بحث در مورد زیرگروههای با مرتبهٔ بیشترین توان عددی اول (قضایای دوم و سوم زیلوف) می‌کشاند .

لم ۱.۵ . *هرگاه گـروه H از مرتبهٔ p^n (p اول) بر مجموعهٔ متناهی S عمل کرده و $S_0 = \{x \in S \mid hx = x \text{ ، به‌ازای هر } h \in H\}$ ، آنگاه $|S| \equiv |S_0| \pmod p$.*

تبصره. از این لم (و نماد S_0) بارها در آینده استفاده خواهد شد .[2]

برهان ۱.۵ . مدار $\bar{x}$ شامل درست یک عنصر است اگر و فقط اگر $x \in S_0$. از اینرو ، S را می‌توان به صورت اجتماع از هم جدایی مانند

$$S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup \cdots \cup \bar{x}_n.$$

---

1. Sylow

۲. *مؤلف از آر . ج . نونکه* R. J. Nunke *به خاطر پیشنهاد این طرز اثبات تشکر دارد .*

نوشت ، که در آن به‌ازای هر i ، $|\bar{x}_i| > 1$. ازاینرو ،

$$|S| = |S_0| + |\bar{x}_1| + |\bar{x}_2| + \cdots + |\bar{x}_n|.$$

اما ، به‌ازای هر i ، $|\bar{x}_i|$ ، p | $|\bar{x}_i|$ ، زیرا $|\bar{x}_i| > 1$ و $|\bar{x}_i| = [H : H_{x_i}]$ ، $|H| = p^n$ راعادمی‌کند . بنابراین ، $|S| \equiv |S_0| \pmod p$.

قضیهٔ ۲۰۵ (کشی[1]) . هرگاه G گروهی متناهی باشدکه‌مرتبه‌اش برعدد اول p بخشپذیر است ، آنگاه G شامل عنصری از مرتبهٔ p می‌باشد .

برهان . (ج . اچ . مک‌کی[2]) .فرض‌کنیم S مجموعهٔ p تاییهایی‌از عناصر گروه به‌صورت $\{(a_1,a_2,\ldots,a_p) \mid a_1a_2\cdots a_p = e \text{ و } a_i \in G\}$ باشد . چون a_p به‌طور منحصر به فرد به صورت $(a_1a_2\cdots a_{p-1})^{-1}$ معین می‌شود ، پس $|S| = n^{p-1}$ ، که در آن $n = |G|$. چون $p \mid n$ ، $|S| \equiv 0 \pmod p$. فرض‌کنیم گروه Z_p به وسیلهٔ جایگشت دوری بر S عمل کند ؛ یعنی ، به‌ازای $k \in Z_p$ ،

$$k(a_1,a_2,\ldots,a_p) = (a_{k+1},a_{k+2},\ldots,a_p,a_1,\ldots,a_k).$$

تحقیق کنید که $(a_{k+1},a_{k+2},\ldots,a_k) \in S$ (از این امر استفاده کنید که در یک گروه $ab = e$ ایجاب می‌کند که $ba = (a^{-1}a)(ba) = a^{-1}(ab)a = e$) .تحقیق کنید که به‌ازای $0,k,k' \in Z_p$ و $x \in S$ ، $0x = x$ و $(k + k')x = k(k'x)$ (نماد جمعی برای عمل گروه بر مجموعه !) . بنابراین ، عمل Z_p بر S تعریف شده است .

اما $(a_1,\ldots,a_p) \in S_0$ اگر و فقط اگر $a_1 = a_2 = \cdots = a_p$ ؛ واضح است که $(e,e,\ldots,e) \in S_0$ ؛ودرنتیجه ، $|S_0| \neq 0$. بنابرلم ۱۰۵ ، $0 \equiv |S| \equiv |S_0| \pmod p$.چون $|S_0| \neq 0$ ، باید دست‌کم p عنصر در S_0 موجود باشد ؛ یعنی ، $a \neq e$ ای باشد به‌طوری که $(a,a,\ldots,a) \in S_0$ ؛ و درنتیجه ، $a^p = e$. چون p اول است ، $|a| = p$.

یک گروه که درآن‌هر عنصر مرتبه‌اش توانی (≥ 0) از عدد اول ثابتی مانند p است یک **p**ـگروه نامیده مـی‌شود . اگـر H زیرگروهی از گروه G و H یک pـگروه باشد ، گوییم H یک **p**ـزیرگروه G است . بخصـوص، به‌ازای هر عدد اول p ، $\langle e \rangle$ یک pـزیرگروه G

---

1. Cauchy 2. J. H. McKay

است ، زیرا $|\langle e\rangle| = 1 = p^0$.

نتیجهٔ ۳۰۵ . گروه متناهی G یک p‌ـگروه است اگر و فقط اگر $|G|$ توانی از p باشد .

برهان . هرگاه G یک pـگروه بوده و q عدد اولی باشد که $|G|$ را عاد می‌کند ، آنگاه طبق قضیهٔ کشی ، G شامل عنصری از مرتبهٔ q است . چون مرتبهٔ هر عنصر G توانی از p است ، $q = p$. از اینرو ، $|G|$ توانی از p است . عکس این مطلب نتیجه‌ای فوری از قضیهٔ لاگرانژ I . ۶.۴ است .

نتیجهٔ ۴۰۵ . مرکز $C(G)$ یک p ـگروه متناهی نابدیهی G دارای بیش از یک عنصر است .

برهان . معادلهٔ رده‌ای G را درنظر می‌گیریم (ر.ک. صفحهٔ ۱۴۱):

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

چون هر $[G : C_G(x_i)] > 1$ و $|G| = p^n$ $(n \geq 1)$ را عاد می‌کند ، p هر $[G : C_G(x_i)]$ و $|G|$ ، و درنتیجه $|C(G)|$ ، را عادخواهدکرد . چون $|C(G)| \geq 1$ ، $C(G)$ دست‌کم دارای p عنصر می‌باشد .

لم ۵۰۵ . هرگاه H یک p‌ـزیرگروه از گروه متناهی G باشد ، آنگاه

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

برهان . فرض کنیم S مجموعهٔ‌هم مجموعه‌های‌چپ H در G بوده‌و H به وسیلهٔ انتقال (چپ) بر S عمل کند . در این صورت ، $|S| = [G : H]$. همچنین ،

$$xH \in S_0 \Leftrightarrow hxH = xH \quad ، \quad \text{به‌ازای هر } h \in H$$

$$\Leftrightarrow x^{-1}hxH = H \quad ، \quad \text{به‌ازای هر } h \in H \Leftrightarrow x^{-1}hx \in H \quad ، \quad \text{به‌ازای هر } h \in H$$

$$\Leftrightarrow x^{-1}Hx = H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H).$$

بنابراین ، $|S_0|$ تعدادهم مجموعه‌های xH به‌ازای $x \in N_G(H)$ است، یعنی، $|S_0| = [N_G(H) : H]$ بنابر لم ۱۰۵ ،

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod{p}.$$

نتیجهٔ ۶۰۵ . هرگاه H یک p-زیرگروه گروه متناهی G باشد به‌طوری که p ، $[G:H]$ را عاد کند ، آنگاه $N_G(H) \neq H$.

برهان . $0 \equiv [G:H] \equiv [N_G(H):H] \pmod{p}$. چون در هر حالت $[N_G(H):H] \geq 1$ ، باید داشته باشیم $[N_G(H):H] > 1$. بنابراین ، $N_G(H) \neq H$.

قضیهٔ ۷۰۵ (قضیهٔ اول زیلوف) . فرض کنیم G گروهی از مرتبهٔ $p^n m$ باشد ، که در آن $n \geq 1$ ، p اول است ، و $(p,m) = 1$. در این صورت ، به‌ازای هر $1 \leq i \leq n$ ، G شامل زیرگروهی از مرتبهٔ p^i است و هر زیرگروه G از مرتبهٔ p^i $(i < n)$ در زیرگروهی از مرتبهٔ p^{i+1} نرمال است .

برهان . چون $p \mid |G|$ ، G شامل عنصری مانند a و لذا ، بنابر قضیهٔ کشی ، شامل زیرگروهی مانند $\langle a \rangle$ از مرتبهٔ p می‌باشد . به‌استقرا عمل کرده ، فرض می‌کنیم H زیرگروهی از G از مرتبهٔ p^i $(1 \leq i < n)$ باشد . در این صورت ، $p \mid [G:H]$ و ، طبق لم ۵۰۵ و نتیجهٔ ۶۰۵ ، H در $N_G(H)$ نرمال است ، و $H \neq N_G(H)$ ، و

$$1 < |N_G(H)/H| = [N_G(H):H] \equiv [G:H] \equiv 0 \pmod{p}.$$

از اینرو ، $p \mid |N_G(H)/H|$ و $N_G(H)/H$ مثل فوق شامل زیرگروهی از مرتبهٔ p است . بنابر نتیجهٔ ۱۲۰۵۰ I ، این گروه به شکل H_1/H است ، که در آن H_1 زیرگروهی از $N_G(H)$ شامل H است . چون H در $N_G(H)$ نرمال است ، H لزوماً در H_1 نرمال می‌باشد . بالاخره

$$|H_1| = |H||H_1/H| = p^i p = p^{i+1}.$$

گوییم زیرگروه P از گروه G **یک p ـ زیرگروه زیلوف** (p اول) است اگر P یک p-زیرگروه ماکزیمال G باشد (یعنی ، $P < H < G$ و pـ گروه بودن H ایجاب می‌کند که $P = H$) . p-زیرگروههای زیلوف همواره وجود دارند ، گرچه ممکن است بدیهی باشند ، و هر p-زیرگروه مشمول یک p-زیرگروه زیلوف است (برای اثبات این در مورد گروههای نامتناهی ، لم زرن لازم است) . قضیهٔ ۷۰۵ نشان می‌دهد که هر گروه متناهی G ، به‌ازای هر عدد اول p ای که $|G|$ را عاد کند ، دارای یک p-زیرگروه زیلوف نابدیهی است . به‌علاوه ، داریم

نتیجهٔ ۸۰۵ . فرض‌کنیم G گروهی‌ازمرتبهٔ $p^n m$ باشد ،که‌درآن p اول‌است ، $n \geq 1$ ، و $(m,p) = 1$. فرض‌کنیم H یک p-زیرگروه G باشد .

(یک) H یک p-زیرگروه زیلوف G است اگر و فقط‌اگر $|H| = p^n$.

(دو) هر مزدوج یک p-زیرگروه زیلوف یک p-زیرگروه زیلوف است .

(سه) هرگاه فقط یک p-زیرگروه زیلوف p-موجود باشد ، آنگاه P در G نرمال است .

طرح برهان . (یک) نتایج I ۰ ۶۰۴ و ۳۰۵ و قضیهٔ ۷۰۵ .

(دو) تمرین I ۰ ۶۰۵ و (یک) . (سه) از (دو) نتیجه می‌شود .

به عنوان عکسی از نتیجهٔ ۸۰۵ (دو) ، داریم

قضیهٔ ۹۰۵ (قضیهٔ دوم‌زیلوف) .هرگاه H یک p-زیرگروه گروه‌متناهی G بوده ، و P یک p-زیرگروه‌زیلوف G باشد ،آنگاه $x \in G$ ی وجوددارد به‌طوری‌که $H < xPx^{-1}$. بخصوص ، هر دو p-زیرگروه زیلوف G مزدوج می‌باشند .

برهان . فرض‌کنیم S مجموعهٔ‌هم‌مجموعه‌های‌چپ P در G بوده‌و H به وسیلهٔ انتقال (چپ) بر S عمل‌کند .بنابر لم ۱۰۵ ، $|S_0| \equiv |S| = [G:P] \pmod p$. اما $p \nmid [G:P]$ ؛ بنابراین ، $|S_0| \neq 0$ ، و $xP \in S_0$ ای وجود دارد .

$$xP \in S_0 \Leftrightarrow hxP = xP \quad \text{، به‌ازای هر } h \in H$$

$$\Leftrightarrow x^{-1}hxP = P \text{ ، به‌ازای هر } h \in H \Leftrightarrow x^{-1}Hx < P \Leftrightarrow H < xPx^{-1}$$

اگر H یک p-زیرگروه باشد ، $|H| = |P| = |xPx^{-1}|$ ؛ و درنتیجه ، $H = xPx^{-1}$.

قضیهٔ ۱۰۵ (قضیهٔ سوم زیلوف) . هرگاه G گروهی متناهی بوده و p اول باشد ، آنگاه تعداد p-زیرگروههای زیلوف G ، $|G|$ را عاد می‌کند و ، به‌ازای $k \geq 0$ ای ، به شکل $kp + 1$ است .

برهان . بنابرقضیهٔ‌دوم زیلوف ،تعداد p-زیرگروههای زیلوف مساوی تعداد مزدوجهای هر یک‌ازآنها ، مثلا " P ، است . امااین عدد مساوی $[G : N_G(P)]$ است ، که بنابر نتیجهٔ

۴.۴ یک مقسوم‌علیه $|G|$ است. فرض کنیم S مجموعهٔ تمام p-زیرگروههای زیلوف G بوده و P به وسیلهٔ تزویج بر S عمل کند. در این صورت، $Q \in S_0$ اگر و فقط اگر به‌ازای هر $x \in P$، $xQx^{-1} = Q$. شرط اخیر برقرار است اگر و فقط اگر $P \cdot P < N_G(Q)$ و Q هر دو p-زیرگروههای زیلوف G و درنتیجه $N_G(Q)$ اندولذا در $N_G(Q)$ مزدوج می‌باشند. اما چون Q در $N_G(Q)$ نرمال است، این فقط وقتی می‌تواند رخ دهد که $Q = P$. بنابراین، $S_0 = \{P\}$ و، طبق لم ۱.۵، $|S| \equiv |S_0| = 1 \pmod p$. لذا، $|S| = kp + 1$.

قضیهٔ ۱۱.۵. هرگاه P یک p-زیرگروه زیلوف گروه متناهی G باشد، آنگاه $N_G(N_G(P)) = N_G(P)$.

برهان. هر مزدوج P یک p-زیرگروه زیلوف G و نیز یک p-زیرگروه زیلوف هر زیرگروه G که شامل آن است می‌باشد. چون P در $N = N_G(P)$ نرمال است، بنابر قضیهٔ ۹.۵، P تنها p-زیرگروه زیلوف N می‌باشد. بنابراین،

$$x \in N_G(N) \Rightarrow xNx^{-1} = N \Rightarrow xPx^{-1} < N \Rightarrow xPx^{-1} = P \Rightarrow x \in N.$$

از اینرو، $N_G(N_G(P)) < N$؛ شمول دیگر واضح است.

تمرینات

۱. هرگاه $N \lhd G$ و $N, G/N$ هر دو p-گروه باشند، آنگاه G نیز p-گروه است.

۲. هرگاه G یک p-گروه متناهی بوده و $H \lhd G$ و $H \neq \langle e \rangle$، آنگاه $H \cap C(G) \neq \langle e \rangle$.

۳. فرض کنید $|G| = p^n$. به‌ازای هر k، $0 \leq k \leq n$، G یک زیرگروه **نرمال** از مرتبهٔ p^k دارد.

۴. هرگاه G یک p-گروه نامتناهی (p اول) باشد، آنگاه به‌ازای هر $n \geq 1$، G زیرگروهی از مرتبهٔ p^n دارد یا $m \in \mathbf{N}^*$ ی هست به‌طوری که هر زیرگروه متناهی G مرتبه‌ای نابیشتر از p^m دارد.

۵. هرگاه P یک p-زیرگروه زیلوف نرمال گروه متناهی G بوده و $f : G \to G$ یک درونریختی باشد، آنگاه $f(P) < P$.

۶. هرگاه H زیرگروه نرمالی از گروه متناهی G و از مرتبهٔ p^k باشد، آنگاه H مشمول هر p-زیرگروه زیلوف G است.

۷ . 2-زیرگروههای زیلوف و 3-زیرگروههای زیلوف S_3 ، S_4 ، S_5 را بیابید .

۸ . اگر هر p-زیرگروه زیلوف گروه متناهی G به‌ازای هر p اول نرمال باشد ، G حاصلضرب مستقیم زیرگروههای زیلوف خود است .

۹ . هرگاه $|G| = p^n q$ ، که در آن p و q اول بوده و $p > q$ ، آنگاه G شامل زیرگروه نرمال منحصر به‌فردی با اندیس q می‌باشد .

۱۰ هرگروه از مرتبهٔ 12 ، 28 ، 56 ، و 200 بایدشامل زیرگروه زیلوف نرمالی باشد ؛ و درنتیجه ، ساده نیست .

۱۱ . در یک گروه ساده از مرتبهٔ 168 چند عنصر از مرتبهٔ 7 وجود دارد .

۱۲ . نشان‌دهیدکه‌هرخودریختی S_4 یک خودریختی‌داخلی است ؛ ولذا ، $S_4 \cong \mathrm{Aut}\, S_4$. [**راهنمایی .** ر.ک. تمرین ۱۰.۴ . هر خودریختی S_4 جایگشتی بر مجموعهٔ $\{P_1,P_2,P_3,P_4\}$ از 3-زیرگروههای‌زیلوف S_4 القامی‌کند . هرگاه $f \in \mathrm{Aut}\, S_4$ دارای این خاصیت باشد که به‌ازای هر i ، $f(P_i) = P_i$ ، آنگاه $f = 1_{S_4}$.]

۱۳ . هر گروه G از مرتبهٔ p^2 (p اول) آبلی است [**راهنمایی .** تمرین ۹.۴ و نتیجهٔ ۴.۵ .]

۶ رده‌بندی گروههای متناهی

ما تمام گروههای مرتبهٔ pq (p,q اول)و تمام گروههای از مرتبهٔ کوچک ($n \leq 15$) را با تقریب یکریختی رده‌بندی می‌کنیم . این نتایج مسلما " خیلی عمیق نیستند ؛ ولی کوششی که صرف آنها می‌شود مشکل تعیین ساختار یک گروه (متناهی) دلخواه را نشان خواهد داد . نتایج این بخش در آینده به کار نخواهند آمد .

حکم ۱۰۶ . فرض کنیم p و q اول بوده و $p > q$. هرگاه $q \nmid p - 1$ ، آنگاه هر گروه از مرتبهٔ pq با گروه دوری Z_{pq} یکریخت است . هرگاه $q \mid p - 1$ ، آنگاه دقیقا " (با تقریب یکریختی) دو گروه متمایز از مرتبهٔ pq وجود دارند ؛ گروه دوری Z_{pq} و گروه غیرآبلی K تولید شده به وسیلهٔ عناصر c و d که

$$|c| = p; \quad |d| = q; \quad dc = c^s d,$$

که در آن $s \not\equiv 1 \pmod p$ و $s^q \equiv 1 \pmod p$.

طرح برهان. گروه‌غیرآبلی K از مرتبهٔ pq با مشخصات حکم وجود دارد (تمرین ۲). فرض کنیم G از مرتبهٔ pq باشد. بنابر قضیهٔ کشی ۲.۵، G شامل عناصری مانند a,b با خاصیت $|a| = p, |b| = q$ است. به‌علاوه، $S = \langle a \rangle$ (بنابرنتیجهٔ ۱.۰.۴ یا با شمارش p-زیرگروههای زیلوف به صورت زیر) در G نرمال است. هم مجموعهٔ bS دارای مرتبهٔ q در گروه G/S است. چون $|G/S| = q$، G/S دوری بـا مولد bS است، $G/S = \langle bS \rangle$. بنابراین، هر عنصر G را می‌توان به شکل $b^i a^j$ نوشت و $G = \langle a,b \rangle$.

تعداد q-زیرگروههای زیلوف مساوی $kq + 1$ است که pq را عاد می‌کند. ازاینرو، مساوی ۱ یا p می‌باشد. هـرگاه مساوی ۱ باشد (که اگر $q \neq p - 1$ چنین است)، آنگاه $\langle b \rangle$ نیز در G نرمال‌است. قضیهٔ لاگرانژ ۱.۰.۶.۴ نشان می‌دهد که $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$. لذا، طبق قضایای ۱.۰.۲.۳، ۱.۰.۶.۸، ۱.۰.۸.۱۰، و تمرین ۱.۰.۵.۸،

$$G = \langle a \rangle \times \langle b \rangle \cong Z_p \oplus Z_q \cong Z_{pq}$$

هـرگاه تعـداد مساوی p باشد (که فقط وقتـی می‌تواند رخ دهد که $p \mid q - 1$)، آنگاه $bab^{-1} = a^r$ (چـون $\langle a \rangle \lhd G$) و $r \not\equiv 1 \pmod p$ (در غیـرایـن صورت، طبق قضیهٔ ۱.۰.۴.۳ (پنج)، G آبلی‌است؛ ودرنتیجه، یک q-زیرگروه‌زیلوف‌منحصر به فرد دارد). چون $bab^{-1} = a^r$، به استقرامعلوم می‌شود که $b^i ab^{-i} = a^{ri}$. بخصوص، به‌ازای $j = q$، $a = a^{rq}$، که طبق قضیهٔ ۱.۰.۴.۳ (پنج) ایجاب می‌کند که $r^q \equiv 1 \pmod p$.

برای‌اتمام برهان بایدنشان دهیم هرگاه $p \mid q - 1$ و G گروه غیرآبلی توصیف شده در بنـد پیش باشد، آنگاه G با K یکریخت است. به چند نتیجه از نظریهٔ اعداد نیاز خواهیم داشت. همنهشتی $x^q \equiv 1 \pmod p$ درست q جواب به پیمانهٔ p دارد (ر.ک. ج. ای. شـوکلی [۵۱ ؛ نتیجهٔ ۱۰.۶، ص ۶۷]). هرگاه r یک جواب و k کوچکترین عددصحیح مثبتی‌باشد که $r^k \equiv 1 \pmod p$، آنگاه $k \mid q$ (ر.ک. ج. ای. شوکلی [۵۱ ؛ قضیـهٔ ۸، ص ۷۰]). در حـالت ما $r \not\equiv 1 \pmod p$، و از آنجا $k = q$. پس‌نتیجه می‌شود که $1, r, r^2, \ldots, r^{q-1}$ همه جـوابهای متمایز به پیمانهٔ p معادلهٔ $x^q \equiv 1 \pmod p$ مـی‌بـاشنـد. درنتیجه، بـه‌ازای t ای $(1 \leq t \leq q - 1)$، $s \equiv r^t \pmod p$. هـرگـاه $b_1 = b^t \in G$، آنگاه $|b_1| = q$. روش بالا (با b_1 به‌جای b) نشان‌می‌دهد که $G = \langle a, b_1 \rangle$؛ هر عنصر G را می‌توان به صورت $b_1^i a^j$ نوشت؛ و $|a| = p$؛ و

$$b_1 ab_1^{-1} = b^t ab^{-t} = a^{rt} = a^s$$ (قضیهٔ ۱.۰.۴.۳ (پنج))

بنابراین، $b_1a = a^1b_1$. تحقیق کنید که نگاشت $G \to K$ داده شده با $a \mapsto c$ و $b_1 \mapsto d$ یکریختی است.

نتیجهٔ ۲.۶ . هرگاه p یک عدد اول فرد باشد، آنگاه هرگروه از مرتبهٔ $2p$ با گروه دوری Z_{2p} یا با گروه دو وجهی D_p یکریخت است.

برهان. حکم ۱.۶ را به‌ازای $q = 2$ به‌کار می‌بریم . اگر G دوری نباشد، شرایط موجود بر s ایجاب می‌کنند که $s \equiv -1 \pmod{p}$. از اینرو، بنابر قضیهٔ I ۴.۳.۰ (پنج)، $G = \langle c,d \rangle$ ، $|d| = 2$ ، $|c| = p$ ، و $dc = c^{-1}d$ ، بنابراین، طبق قضیهٔ I ۱۳.۶.۰ ، $G \cong D_p$.

حکم ۳.۶ . درست (با تقریب یکریختی) دو گروه غیرآبلی از مرتبهٔ 8 وجود دارند: گروه چهارتایی Q_8 و گروه دو وجهی D_4 .

تبصره. گروه چهارتایی Q_8 در تمرین I ۳.۲.۰ توصیف شده است.

طرح برهان ۳.۶ . تحقیق کنید که $D_4 \ncong Q_8$ (تمرین ۱۰) . هرگاه گروه G از مرتبهٔ 8 غیرآبلی باشد، آنگاه نمی‌تواند عنصری از مرتبهٔ 8 داشته یا مرتبهٔ هر عنصر غیرهمانی آن 2 باشد (تمرین I ۱۳.۱.۰) . ازاینرو، G شامل عنصری مانند a از مرتبهٔ 4 است. گروه $\langle a \rangle$ با اندیس 2 نرمال است . $b \notin \langle a \rangle$ را اختیار می‌کنیم . پس $b^2 \in \langle a \rangle$. زیرا $|G/\langle a \rangle| = 2$. نشان دهید که تنها حالات ممکن عبارتند از $b^2 = a^2$ یا $b^2 = e$. چون $\langle a \rangle$ در G نرمال است، $bab^{-1} \in \langle a \rangle$ ؛ تنها حالت ممکن عبارت است از $bab^{-1} = a^3 = a^{-1}$. پس نتیجه می‌شود که هر عنصر G را می‌توان به شکل b^ia^j نوشت . از اینرو، $G = \langle a,b \rangle$. در یک حالت، طبق تمرین I ۱۴.۴.۰ ، داریم $|a| = 4$ ، $b^2 = a^2$ ، $ba = a^{-1}b$ ، و $G \cong Q_8$ ؛ در حالت دیگر، بنابر قضیهٔ I ۱۳.۶.۰ ، داریم $|a| = 4$ ، $|b| = 2$ ، $ba = a^{-1}b$ ، و $G \cong D_4$.

حکم ۴.۶ . درست (با تقریب یکریختی) سه گروه غیرآبلی متمایز از مرتبهٔ 12 وجود دارند: گروه دو وجهی D_6 ، گروه متناوب A_4 ، و گروه T تولید شده به وسیلهٔ عناصر

a,b به‌طوری که $|a| = 6$ ، $b^2 = a^3$ ، و $ba = a^{-1}b$.

طرح برهان. تحقیق کنیدکه گروه T از مرتبهٔ 12 به صورت فوق وجود دارد (تمرین ۵) و هیچ دو تا از D_6, A_4, T یکریخت نیستند (تمرین ۶) . اگر G یک گروه غیرآبلی از مرتبهٔ 12 باشد ، P رایک 3-زیرگروه‌زیلوف G می‌گیریم .دراین‌صورت ، $|P| = 3$ و $[G : P] = 4$. بنابر حکم ۸.۴ ، یک همریختی مانند $f : G \to S_4$ وجود دارد که هسته‌اش K مشمول P است ، کـه از آنجا K مساوی P یا $\langle e \rangle$ می‌باشد . اگر $K = \langle e \rangle$ ، f یک تکریختی است و G با زیرگروهی‌ازمرتبهٔ 12 از S_4 یکریخت‌است ،که‌طبق‌قضیهٔ I . ۸.۶ باید A_4 باشد . در غیراین‌صورت ، $K = P$ و P در G نرمال‌است .دراین حالت ، P ، 3-زیرگروه‌زیلوف منحصربه فردمی‌باشد .از اینرو ، G فقط شامل دو عنصر از مرتبهٔ 3 است . هرگاه c یکی از اینهاباشد ،آنگاه $[G : C_G(c)]$ مساوی 1 یا 2 است ، زیرا $[G : C_G(c)]$ تعداد مزدوجهای c بوده‌و هر مزدوج c از مرتبهٔ 3 می‌باشد . از اینرو ، $C_G(c)$ گروهی از مرتبهٔ 12 یا 6 است . در هر حالت ، بنابر قضیهٔ کشی ، $d \in C_G(c)$ ای از مرتبهٔ 2 وجود دارد . تحقیق کنید که $|cd| = 6$.

فرض‌کنیم $a = cd$ ؛ پس $\langle a \rangle$ در G نرمال اسـت‌و $|G/\langle a \rangle| = 2$. از اینرو ، عنصری مانند $b \in G$ وجود دارد به‌طوری که $b \notin \langle a \rangle$ ، $b \neq e$ ، $b^2 \in \langle a \rangle$ ، و $bab^{-1} \in \langle a \rangle$. چون G غیرآبلی‌است‌و $|a| = 6$ ، $bab^{-1} = a^5 = a^{-1}$ تنهاحالت‌ممکن‌است ؛ یعنی ، $ba = a^{-1}b$. برای $b^2 \in \langle a \rangle$ شش حالت‌ممکن‌است . $b^2 = a^2$ یا $b^2 = a^4$ به‌تناقض ختم می‌شوند ؛ $b^2 = a$ یا $b^2 = a^5$ ایجـاب می‌کند کـه $|b| = 12$ و G آبلی باشد . بنابراین ، تنها حالات ممکن عبارتند از

(یک) $|a| = 6; b^2 = e; ba = a^{-1}b$ ، که از آنجـا ، طبق قضیهٔ I ۱۳.۶ ، $G \cong D_6$ ؛

(دو) $|a| = 6; b^2 = a^3; ba = a^{-1}b$ ،که از آنجا ، طبق تمرین ۵ (ب) ، $G \cong T$.

جدول زیـر تمام گـروههای متمایز از مرتبهٔ کوچک را (با تقریب یکریختی) لیست کرده است . 14 گروه‌متمایز ازمرتبهٔ 16 و 51 گروه از مرتبهٔ 32 وجود دارند ؛ ر.ک . ام . هال[1] و ج . کا . سینیور[2] [۱۶] .هنوز هیچ فرمولی‌که‌تعداد گروههای متمایز از مرتبهٔ n ،

---

1. M. Hall 2. J.K. Senior

به‌ازای هر n ، را بدهد معلوم نشده است .

مرتبه	گروههای متمایز	مراجعه
1	$\langle e \rangle$	. . .
2	Z_2	تمرین I . ۳۰۴
3	Z_3	تمرین I . ۳۰۴
4	$Z_2 \oplus Z_2$, Z_4	تمرین I . ۵۰۴
5	Z_5	تمرین I . ۳۰۴
6	Z_6, D_3	نتیجهٔ ۲۰۶
7	Z_7	تمرین I . ۳۰۴
8	$Z_2 \oplus Z_2 \oplus Z_2$, $Z_2 \oplus Z_4$, Z_8, Q_8, D_4	قضیهٔ ۱۰۲ و حکم ۳۰۶
9	$Z_3 \oplus Z_3$, Z_9	تمرین ۱۳۰۵ و قضیهٔ ۱۰۲
10	Z_{10}, D_5	نتیجهٔ ۲۰۶
11	Z_{11}	تمرین I . ۳۰۴
12	$Z_2 \oplus Z_6$, Z_{12}, A_4, D_6, T	قضیهٔ ۱۰۲ و حکم ۴۰۶
13	Z_{13}	تمرین I . ۳۰۴
14	Z_{14}, D_7	نتیجهٔ ۲۰۶
15	Z_{15}	حکم ۱۰۶

تمرینات

۱ . فرض کنید G و H گروه بوده و $\theta : H \to \operatorname{Aut} G$ یک همریختی باشد . همچنین ، $G \times_\theta H$ مجموعهٔ $G \times H$ با عمل دوتایی زیر باشد ؛

$$(g,h)(g',h') = (g[\theta(h)(g')],hh').$$

نشان دهیدکه $G \times_\theta H$ یک‌گروه‌باعنصرهمانی (e,e) است‌و $(g,h)^{-1} = (\theta(h^{-1})(g^{-1}),h^{-1})$. $G \times_\theta H$ حاصل‌ضرب نیم مستقیم G و H نامیده می‌شود .

۲ . فرض کنید $C_p = \langle a \rangle$ و $C_q = \langle b \rangle$ گروههای دوری (ضربی)و به‌ترتیب‌از مرتبهٔ اول p و q باشند به‌طوری که $p > q$ و $q \mid p - 1$. فرض‌کنید s عددی صحیح باشد به طوری‌که $s \not\equiv 1 \pmod p$ و $s^q \equiv 1 \pmod p$ ، کـه ایجاب می‌کند $s \not\equiv 0 \pmod p$. نظریهٔ مقدماتی اعداد نشان می‌دهد که چنین s ی وجود دارد (ر . ک . ج . ای .

شوکلی [۵۱ : نتیجهٔ ۱۰۶ ، ص ۶۷] .

(آ) نگاشت $\alpha : C_p \to C_p$ داده شده با $a^i \mapsto a^{si}$ یک خودریختی است .

(ب) نگاشت $\theta : C_q \to \mathrm{Aut}\, C_p$ داده شده با $\theta(b^i) = \alpha^i$ (α مثل‌قسمت (آ)) یک همریختی است $(\alpha^0 = 1_{C_p})$.

(پ) هرگاه به‌جای (a,e) بنویسیم a و به جای (e,b) بنویسیم b ، آنگاه گروه $C_p \times_\theta C_q$ (ر.ک. تمرین ۱) یک گروه از مرتبهٔ pq است ، که به وسیلهٔ a و b تحت روابط زیر تولید می‌شود : $|a| = p$ ، $|b| = q$ ، $ba = a^s b$ ، که در آن $s \not\equiv 1 \pmod p$ ، و $s^q \equiv 1 \pmod p$. گروه $C_p \times_\theta C_q$ **گروه ماوراء دوری** نامیده می‌شود .

۳ . مجموعهٔ $G = \{\pm 1, \pm i, \pm j, \pm k\}$ با ضرب

$$i^2 = j^2 = k^2 = -1;\ ij = k;\ jk = i,\ ki = j;\ ji = -k,\ kj = -i,\ ik = -j,$$

و قواعد معمولی ضرب در ± 1 را درنظر بگیرید . نشان دهید G گروهی است که با گروه چهارتایی Q_8 یکریخت است .

۴ . مرکز گروه چهارتایی Q_8 چیست ؟ نشان دهید که $Q_8/C(Q_8)$ آبلی است .

۵ . (آ) نشان دهید که زیرگروهی غیرآبلی مانند T از $S_3 \times Z_4$ با مرتبهٔ 12 وجود دارد که با عناصر a,b صادق در $|a| = 6,\ a^3 = b^2,\ ba = a^{-1}b$ تولید می‌شود .

(ب) هرگروه از مرتبهٔ 12 با مولدهای a,b صادق در $|a| = 6,\ a^3 = b^2,\ ba = a^{-1}b$ با T یکریخت است .

۶ . هیچ دو تا از D_6 ، A_4 ، و T ، که T گروه مرتبهٔ 12 توصیف شده در حکم ۴.۶ و تمرین ۵ است ، با هم یکریخت نیستند .

۷ . هرگاه G گروهی غیرآبلی از مرتبهٔ p^3 (p اول) باشد ، آنگاه مرکز G زیرگروه تولید شده به وسیلهٔ تمام عناصر به شکل $aba^{-1}b^{-1}$ $(a,b \in G)$ می‌باشد .

۸ . فرض کنید p عدد اول **فردی** باشد . ثابت کنید حداکثر دو گروه غیرآبلی از مرتبهٔ p^3 وجود دارند . [یکی دارای مولدهای a,b است که در روابط زیر صدق می‌کند $|a| = p^2;\ |b| = p;\ b^{-1}ab = a^{1+p}$ ؛ دیگری دارای مولدهای a,b,c صادق در روابط $|a| = |b| = |c| = p;\ c = a^{-1}b^{-1}ab;\ ca = ac;\ cb = bc$ می‌باشد .]

۹ . تمام گروههای مرتبهٔ 18 را با تقریب یکریختی رده‌بندی کنید . همین کار را درمورد مراتب 20 و 30 انجام دهید .

۱۰ . نشان‌دهیدکه D_4 با Q_8 یکریخت‌نیست . [**راهنمایی .** عناصرمرتبهٔ 2 رابشمارید.]

۷ گروههای پوچ‌توان و حلپذیر

شرایط‌زیر را بر گروه متناهی G در نظر می‌گیریم .

(یک) G حاصل‌ضرب مستقیم زیرگروههای زیلوف خود است .

(دو) هرگاه m ، $|G|$ را عاد کند ، آنگاه G زیرگروهی از مرتبهٔ m دارد .

(سه) هرگاه $|G| = mn$ و $(m,n) = 1$ ، آنگاه G زیرگروهی از مرتبهٔ m دارد . شرایط (دو) و (سه) را می‌توان تعدیلهایی از قضیهٔ اول زیلوف دانست . به‌آسانی می‌توان نشان‌دادکه (دو) $\Rightarrow$ (یک) و بوضوح (سه) $\Rightarrow$ (دو) . این امر که هر گروه آبلی متناهی در (یک) صدق می‌کندنتیجهٔ‌ساده‌ای‌ازقضیهٔ ۲۰۲ است . هر p-گروه بداهتا " در (یک) صدق می‌کند . از آن سو ، A_4 در (سه) صدق می‌کند ولی در (دو) صدق نمی‌کند ، و S_3 در (دو) صدق‌می‌کندولی در (یک) صدق نمی‌کند (تمرین ۱) . باتوجه به نتایج نسبتا " جالبی کـه تاکنون برای p-گروههای آبلی متناهی به دست آمده‌اند ، رده‌های گروههای به‌ترتیب‌صادق‌در (یک) ، (دو) ، و (سه) نامزدهای‌مناسبی برای بررسی به نظر می‌رسند . ما توجه خود را به گروههایی معطوف می‌کنیم که در (یک) یا (سه) صدق می‌نمایند .

ابتدا گروههای پوچ‌توان و حلپذیر را برحسب "سری نرمالی" از زیرگروهها تعریف می‌کنیم . در حـالت گـروههای متناهی ، گروههای پوچ‌توان به‌وسیلهٔ شرط (یک) (حکم ۵۰۷) و گروههای حلپذیر به وسیلـهٔ شـرط (سه) (حکم ۱۴۰۷) مشخص می‌شوند . این روش نیزنشان می‌دهد که رابطه‌ای بین گروههای پوچ‌توان و حلپذیر و تعویضپذیری وجود دارد . مشخصات دیگر گروههای پوچ‌توان و حلپذیر در بخش ۸ داده می‌شوند .

بحث گروههای‌حلپذیرصرفا "درنظریهٔ گروههاست . اما ، از نظر تاریخی ، گروههای حلپذیر ابتدا در رابطه‌بامسئلهٔ تعیین ریشه‌های یک چندجمله‌ای با ضرایب در یک میدان ظاهر شدند (ر.ک. بخش ۹۰۷) .

فرض کنیـم G یک گـروه باشد . $C(G)$ ، مرکز گـروه G ، یک زیرگروه نرمال است (نتیجـهٔ ۷۰۴) . فـرض کنیـم $C_2(G)$ نقش معکـوس $C(G/C(G))$ تحت تصویر کانونی $G \to G/C(G)$ باشد.در ایـن صورت طبق (برهان) قضیهٔ ۱۱۰۵ . I ، $C_2(G)$ در G نرمال است و شامل $C(G)$ می‌باشد .این فرایندرا با تعریف استقرایی زیر ادامه می‌دهیم :

$C_1(G) = C(G)$ و $C_i(G)$ را نقش معکوس $C(G/C_{i-1}(G))$ تحت تصویر کانونی $G \to G/C_{i-1}(G)$

اختیار می‌کنیم. دراین‌صورت، دنباله‌ای از زیرگروههای نرمال G، **به نام سری مرکزی افزایشی** G، مانند $\langle e\rangle < C_1(G) < C_2(G) < \cdots$ به‌دست می‌آوریم.

تعریف ۱۰۷. گروه G **پوچ‌توان** است اگر به‌ازای n ی، $C_n(G) = G$.

هر گروه آبلی G پوچ‌توان است، زیرا $G = C(G) = C_1(G)$.

قضیهٔ ۲۰۷. هر p-گروه متناهی پوچ‌توان است.

برهان. G وتمام خارج قسمتهای نا بدیهی آن p-گروهند؛ و لذا، طبق نتیجهٔ ۴۰۵، دارای مراکز نابدیهی می‌باشند. این ایجاب می‌کند که هرگاه $G \neq C_i(G)$، آنگاه $C_i(G)$ اکیدا" مشمول $C_{i+1}(G)$ باشد. چون G متناهی است، $C_n(G)$ باید به‌ازای n ی مساوی G باشد.

قضیهٔ ۳۰۷. حاصل‌ضرب مستقیم تعدادی متناهی گروه پوچ‌توان پوچ‌توان است.

برهان. برای راحتی فرض کنیم $G = H \times K$؛ برهان در مورد عوامل بیش از دو مشابه است. به استقرا فرض کنیم $C_i(G) = C_i(H) \times C_i(K)$ (حالت $i = 1$ واضح است). فرض کنیم π_H بروریختی کانونی $H \to H/C_i(H)$ باشد و به همین نحو در مورد π_K. تحقیق کنید که بروریختی کانونی $\varphi : G \to G/C_i(G)$ ترکیب زیر است:

$$G = H \times K \xrightarrow{\pi} H/C_i(H) \times K/C_i(K) \xrightarrow{\psi} \frac{H \times K}{C_i(H) \times C_i(K)} = \frac{H \times K}{C_i(H \times K)} = G/C_i(G),$$

که در آن $\pi = \pi_H \times \pi_K$ (قضیهٔ I ۱۰۸۰۱۰)، و ψ یکریختی نتیجهٔ I ۱۱۰۸۰ می‌باشد. درنتیجه،

$$\begin{aligned} C_{i+1}(G) &= \varphi^{-1}[C(G/C_i(G))] = \pi^{-1}\psi^{-1}[C(G/C_i(G))] \\ &= \pi^{-1}[C(H/C_i(H) \times K/C_i(K))] \\ &= \pi^{-1}[C(H/C_i(H)) \times C(K/C_i(K))] \\ &= \pi_H{}^{-1}[C(H/C_i(H))] \times \pi_K{}^{-1}[C(K/C_i(K))] \\ &= C_{i+1}(H) \times C_{i+1}(K). \end{aligned}$$

لذا، مرحلهٔ استقرا ثابت شده است و به‌ازای هر i ، $C_i(G) = C_i(H) \times C_i(K)$. چون H,K پوچ‌توانند، $n \in \mathbf{N}^*$ ی هست به‌طوری که $C_n(H) = H$ و $C_n(K) = K$ ، که از آنجا $C_n(G) = H \times K = G$. بنابراین، G پوچ‌توان است.

لم ۴۰۷ . هرگاه H یک زیرگروه حقیقی از گروه پوچ‌توان G باشد، آنگاه H یک زیرگروه حقیقی نرمال‌ساز آن $N_G(H)$ است.

برهان. فرض کنیم $C_0(G) = \langle e \rangle$ و n بزرگترین اندیسی باشد که $C_n(G) < H$ (این n وجود دارد، زیرا G پوچ‌توان و H یک زیرگروه حقیقی است) . $a \in C_{n+1}(G)$ را طوری اختیار می‌کنیم که $a \notin H$. در این صورت، به‌ازای هر $h \in H$ ،

$$C_n ah = (C_n a)(C_n h) = (C_n h)(C_n a) = C_n ha$$

در $G/C_n(G)$ است، زیرا $C_n a$ ، طبق تعریف $C_{n+1}(G)$ ، در مرکز می‌باشد. لذا، $ah = h'ha$ ، که در آن $h' \in C_n(G) < H$. ازاینرو، $aha^{-1} \in H$ و $a \in N_G(H)$. چون $a \notin H$ ، H یک زیرگروه حقیقی $N_G(H)$ می‌باشد.

حکم ۵۰۷ . یک گروه متناهی پوچ‌توان است اگر و فقط اگر حاصل‌ضرب مستقیم زیرگروههای زیلوف خود باشد.

برهان. هرگاه G حاصل‌ضرب مستقیم p-زیرگروههای زیلوف خود باشد، آنگاه G ، طبق قضیهٔ ۲۰۷ و ۳۰۷ ، پوچ‌توان است. هرگاه G پوچ‌توان بوده و P ، به‌ازای عدد اولی مانند p یک p-زیرگروه زیلوف G باشد، آنگاه $P = G$ (و مقصود حاصل است) یا P زیرگروهی حقیقی از G است. در حالت دوم، P ، طبق لم ۴۰۷ ، یک زیرگروه حقیقی $N_G(P)$ است. چون، طبق قضیهٔ ۱۱۰۵ ، $N_G(P)$ نرمال‌ساز خود است، باید، طبق لم ۴۰۷ ، داشته باشیم $N_G(P) = G$. لذا، P در G نرمال است؛ و درنتیجه، بنابر قضیهٔ ۹۰۵ ، p-زیرگروه زیلوف منحصر به فرد G می‌باشد. فرض کنیم $|G| = p_1^{n_1} \cdots p_k^{n_k}$ (p_i ها اعداد اول متمایزی هستند و $n_i > 0$) و نیز $P_1, P_2, \ldots, P_k$ زیرگروههای زیلوف (نرمال حقیقی) نظیر از G باشند. چون به‌ازای هر i ، $|P_i| = p_i^{n_i}$ ، به‌ازای $i \neq j$ ، $P_i \cap P_j = \langle e \rangle$. بنابر قضیهٔ I ۳۰۵ ، به‌ازای هر $(i \neq j)$ $x \in P_i, y \in P_j$ ، $xy = yx$.

پس نتیجه می‌شود که به‌ازای هر i ، $P_1P_2\cdots P_{i-1}P_{i+1}\cdots P_k$ زیرگروهی است که در آن مرتبهٔ هر عنصر $p_1^{n_1}\cdots p_{i-1}^{n_{i-1}}p_{i+1}^{n_{i+1}}\cdots p_k^{n_k}$ را عاد می‌کند. در نتیجه،

$$P_1P_2\cdots P_k = P_1\times\cdots\times P_k \quad \text{و} \quad P_i\cap(P_1\cdots P_{i-1}P_{i+1}\cdots P_k)=\langle e\rangle$$

چون

$$|G| = p_1^{n_1}\cdots p_k^{n_k} = |P_1\times\cdots\times P_k| = |P_1\cdots P_k|$$

باید داشته باشیم $G = P_1P_2\cdots P_k = P_1\times\cdots\times P_k$.

نتیجهٔ ۶.۷ . هرگاه G یک گروه پوچ‌توان متناهی بوده و m ، |G| را عاد کند ، آنگاه G زیرگروهی از مرتبهٔ m دارد .

برهان . تمرین .

تعریف ۷.۷ . فرض کنیم G گروه باشد . زیرگروه G تولید شده به وسیلهٔ مجموعهٔ $\{aba^{-1}b^{-1} \mid a,b\in G\}$ **زیرگروه تعویضگر** G نام دارد و با G' نموده می‌شود .

عناصر $aba^{-1}b^{-1}$ $(a,b\in G)$ را **تعویضگر** می‌نامند . تعویضگرها فقط G' را تولید می‌کنند؛ درنتیجه ، G' ممکن است شامل عناصری باشد که تعویضگر نیستند . G آبلی است اگر و فقط اگر $G'=\langle e\rangle$. به یک معنی ، G' تفاوت G از یک گروه آبلی را می‌سنجد .

قضیهٔ ۸.۷ . هرگاه G گروه باشد ، آنگاه G' زیرگروه نرمالی از G است و G/G' آبلی می‌باشد . هرگاه N زیرگروه نرمالی از G باشد ، آنگاه G/N آبلی است اگر و فقط اگر N شامل G' باشد .

برهان . فرض کنیم $f : G\to G$ یک خودریختی باشد . در این صورت ،

$$f(aba^{-1}b^{-1}) = f(a)\,f(b)\,f(a)^{-1}f(b)^{-1}\in G'.$$

پس نتیجه می‌شود که $f(G')<G'$. بخصوص، هرگاه f خودریختی داده شده به وسیلهٔ تزویج به وسیلهٔ $a\in G$ باشد ، آنگاه $aG'a^{-1}=f(G')<G'$ ، که از آنجا ،طبق قضیهٔ ۱.۵.۱۰، G' در G نرمال است . چون $(ab)(ba)^{-1}=aba^{-1}b^{-1}\in G'$ ، $abG'=baG'$ ؛ و درنتیجه ،

G/G' آبلی است. هرگاه G/N آبلی باشد، آنگاه به‌ازای هر $a,b \in G$ ، $abN = baN$ ، که از آنجا $ab(ba)^{-1} = aba^{-1}b^{-1} \in N$. بنابراین، N شامل‌تمام تعویضگرهاست و $G' < N$. عکس مطلب آسان است.

فرض‌کنیم G گروه‌و $G^{(1)}$ مساوی G' باشد. به‌ازای $i \geq 1$ ، $G^{(i)}$ را با $G^{(i)} = (G^{(i-1)})'$ تعریف می‌کنیم. $G^{(i)}$ **زیرگروه مشتق** i ام G نامیده می‌شود. از آنجا دنباله‌ٔ زیر از زیرگروههای G به‌دست می‌آید که هریک در ماقبل خود نرمال است: $G > G^{(1)} > G^{(2)} > \ldots$. درواقع، هر $G^{(i)}$ یک زیرگروه نرمال G است (تمرین ۱۳).

تعریف ۹.۷ . گوییم گروه G **حلپذیر** است اگر به‌ازای n ی، $G^{(n)} = \langle e \rangle$.

هر گروه آبلی بداهتا" حلپذیر است. به‌طورکلی، داریم

حکم ۱۰.۷ . *هر گروه پوچ‌توان حلپذیر است.*

برهان. چون طبق تعریف $C_i(G)$ ، $C_i(G)/C_{i-1}(G) = C(G/C_{i-1}(G))$ آبلی است، به‌ازای هر $i > 1$ ، $C_i(G)' < C_{i-1}(G)$ و $C_1(G)' = C(G)' = \langle e \rangle$. به‌ازای n ی، $G = C_n(G)$. بنابراین، $C(G/C_{n-1}(G)) = C_n(G)/C_{n-1}(G) = G/C_{n-1}(G)$ آبلی است؛ و درنتیجه، $G^{(2)} = G^{(1)\prime} < C_{n-1}(G)' < C_{n-2}(G)$. بنابراین، $G^{(1)} = G' < C_{n-1}(G)$ ؛ به همین نحو،

$$G^{(3)} < C_{n-2}(G)' < C_{n-3}(G); \ldots, G^{(n-1)} < C_2(G)' < C_1(G); G^{(n)} < C_1(G)' = \langle e \rangle.$$

از اینرو، G حلپذیر است.

قضیهٔ ۱۱.۷ . **(یک)** *هر زیرگروه و هر نقش همریخت یک گروه حلپذیر حلپذیر است.*
(دو) *هرگاه N زیرگروه نرمالی از گروه G باشد به‌طوری که N و G/N حلپذیر باشند، آنگاه G حلپذیر است.*

طرح برهان. (یک) اگر $f : G \to H$ یک همریختی [بروریختی] باشد، تحقیق کنید به‌ازای هر i ، $f(G^{(i)}) < H^{(i)}[f(G^{(i)}) = H^{(i)}]$. فرض‌کنیم f یک بروریختی بوده، و G

حلپذیر باشد. در این صورت، به‌ازای n ی، $\langle e \rangle = f(e) = f(G^{(n)}) = H^{(n)}$، که از آنجا H حلپذیر است. برهان در مورد یک زیرگروه مشابه است.

(دو) فرض کنیم $f : G \to G/N$ برووریختی کانونی باشد. چون G/N حلپذیر است، به‌ازای n ی، $f(G^{(n)}) = (G/N)^{(n)} = \langle e \rangle$. از اینرو، $G^{(n)} < \operatorname{Ker} f = N$. چون طبق (یک)، $G^{(n)}$ حلپذیر است، $k \in \mathbf{N}^*$ ای هست بطوری که $G^{(n+k)} = (G^{(n)})^{(k)} = \langle e \rangle$. بنابراین، G حلپذیر می‌باشد.

نتیجهٔ ۱۲.۷. *هرگاه $n \geq 5$، آنگاه گروه متقارن S_n حلپذیر نیست.*

برهان. هرگاه S_n حلپذیربود، A_n حلپذیرمی‌شد. چون A_n غیرآبلی‌است، $A_n' \neq (1)$. و چون A_n' در A_n نرمال است (قضیهٔ ۸.۷) و A_n ساده می‌باشد (قضیهٔ I ۱۰.۶۰)، باید داشته باشیم $A_n' = A_n$. بنابراین، به‌ازای هر $i \geq 1$، $A_n^{(i)} = A_n \neq (1)$، که از آنجا A_n حلپذیر نمی‌باشد.

تذکر. باقی‌ماندهٔ این بخش در آینده به کار نمی‌آید.

برای اثبات تعمیم قضایای زیلوف برای گروههای حلپذیر متناهی (به صورت مذکور در بند اول این بخش) به چند تعریف و لم نیاز خواهیم داشت. گوییم زیرگروه H از گروه G *مشخص* [*کاملا*" *پایا*] است اگر به‌ازای هرخودریختی [درونریختی] $f : G \to G$، $f(H) < H$. واضح است که هرزیرگروه کاملا" پایا مشخص است و هر زیرگروه مشخص نرمال است (زیرا تزویج یک خودریختی است). یک *زیرگروه نرمال مینیمال* گروه G یک زیرگروه نرمال نابدیهی است که شامل هیچ زیرگروه حقیقی نرمال در G نمی‌باشد.

لم ۱۳.۷. *فرض کنیم N زیرگروه نرمالی از گروه متناهی G بوده و H زیرگروهی از G باشد.*

(یک) هرگاه H یک زیرگروه مشخص N باشد، آنگاه H در G نرمال است.

(دو) هر p-زیرگروه زیلوف نرمال G کاملا" پایاست.

(سه) هرگاه G حلپذیر بوده و N یک زیرگروه نرمال مینیمال باشد، آنگاه N، به‌ازای

عدد اولی مانند p ، یک p-گروه آبلی می‌باشد .

برهان . (یک) چون به‌ازای هر $a \in G$ ، $aNa^{-1} = N$ ، تزویج به وسیلهٔ a یک خودریختی N است . چون H در N مشخص است ، به‌ازای هر $a \in G$ ، $aHa^{-1} < H$. از اینرو ، طبق قضیهٔ ۱۰۵ . I ، H در G نرمال است .

قسمت (دو) را به عنوان تمرین می‌گذاریم . (سه) به‌آسانی معلوم می‌شود که N' در N کاملا" پایاست ، که از آنجا ، طبق قسمت (یک) ، N' در G نرمال است . چون N یک زیرگروهٔ نرمال مینیمال است ، $N' = \langle e \rangle$ یا $N' = N$. چون N حلپذیر است (قضیهٔ ۱۱۰۷) ، $N' \neq N$. از اینرو ، $N' = \langle e \rangle$ و N یک گروه آبلی نابدیهی است . فرض کنیم P یک p-زیرگروه‌زیلوف‌نابدیهی N به‌ازای p ی اولی باشد . چون N آبلی است ، P در N نرمال است ؛ و درنتیجه ، طبق (دو) ، در N کاملا" پایاست . درنتیجه ، طبق (یک) ، P در G نرمال‌است . چون N مینیمال و P نابدیهی است ، باید داشته باشیم $P = N$.

حکم ۱۴۰۷ . (پی .هال[1]) فرض‌کنیم G یک گروه حلپذیر متناهی از مرتبهٔ mn باشد ، که $(m,n) = 1$. در این صورت ،

(یک) G شامل زیرگروهی از مرتبهٔ m است ؛

(دو) هر دو زیرگروه G از مرتبهٔ m مزدوجند ؛

(سه) هر زیرگروه G از مرتبهٔ k ، که $k \mid m$ ، مشمول زیرگروهی از مرتبهٔ m است .

چند تبصره . اگر m توان اولی باشد ، حکم فوق‌چند نتیجهٔ موجود در قضایای زیلوف را مجددا" بیان می‌کند . پی .هال همچنین عکس (یک) را ثابت کرد : هرگاه G گروهی متناهی باشد به‌قسمی که هروقت $|G| = mn$ و $(m,n) = 1$ ، G زیرگروهی از مرتبهٔ m داشته باشد ، آنگاه G حلپذیر است . اثبات از حوصلهٔ این کتاب خارج است (ر .ک . ام .هال [۱۵] ؛ ص ۱۴۳) .

برهان ۱۴۰۷ . اثبات به استقرا بر $|G|$ است ، مرتبه‌های نابیشتر از 5 بدیهی‌اند . دو حالت وجود دارند .

---

1. P. Hall

حالت ۱. زیرگروه نرمال حقیقی H از G وجود دارد که مرتبه‌اش بر n بخشپذیر نیست.

(یک) $|H| = m_1n_1$ ، که در آن $m_1 \mid m$ ، $n_1 \mid n$ ، و $n_1 < n$. G/H یک گروه حلپذیر از مرتبهٔ $(m/m_1)(n/n_1) < mn$ است با $(m/m_1, n/n_1) = 1$. لذا، بنابر استقرا، G/H شامل زیرگروه A/H از مرتبهٔ (m/m_1) است (که در آن A زیرگروهی از G است ــ ر.ک. نتیجهٔ I ۱۲۰۵ ۰) . در این صورت،

$$|A| = |H|[A : H] = (m_1n_1)(m/m_1) = mn_1 < mn.$$

A حلپذیر است (قضیهٔ ۱۱۰۷) و، بنابر استقرا، شامل زیرگروهی از مرتبهٔ m می‌باشد.

(دو) فرض کنیم B,C زیرگروههای G از مرتبهٔ m باشند. چون H در G نرمال است، HB زیرگروهی است (قضیهٔ I ۳۰۵۰) که مرتبه‌اش k لزوماً $|G| = mn$ را عاد می‌کند. چون

$$k = |HB| = |H||B|/|H \cap B| = m_1n_1m/|H \cap B|,$$

داریم $k|H \cap B| = m_1n_1m$ ، که از آنجا $k \mid m_1n_1m$. چون $(m_1,n) = 1$ ، اعداد صحیحی مانند x,y وجود دارند به طوری که $m_1x + ny = 1$ ؛ و در نتیجه، $mm_1x + mn_1y = mn_1$. در نتیجه، $k \mid mn_1$. بنابر قضیهٔ لاگرانژ I ۶۰۴۰ ، $m = |B|$ و $m_1n_1 = |H|$ ، k را عاد می‌کنند. لذا، $(m,n) = 1$ ایجاب می‌کند که $mn_1 \mid k$. بنابراین، $k = mn_1$ ؛ به همین نحو، $|HC| = mn_1$. لذا، HB/H و HC/H زیرگروههای G/H از مرتبهٔ m/m_1 اند. اینها، بنا بر استقرا، مزدوجند: به‌ازای $x \in G$ ی (x که هم مجموعهٔ $x \in G/H$ است)، $x(HB/H)x^{-1} = HC/H$. پس نتیجه می‌شود که $xHBx^{-1} = HC$. درنتیجه، xBx^{-1} و C زیرگروههای HC از مرتبهٔ m اند؛ و لذا، طبق استقرا، در HC مزدوج می‌باشند. از اینرو، B و C در G مزدوج می‌باشند.

(سه) هرگاه زیرگروه K از G دارای مرتبهٔ k باشد که m را عاد می‌کند، آنگاه $HK/H \cong K/H \cap K$ مرتبه‌ای دارد که k را عاد می‌کند. چون HK/H زیرگروه G/H است، مرتبه‌اش $|G/H| = (m/m_1)(n/n_1)$ را نیز عاد می‌کند. $(k,n) = 1$ ایجاب می‌کند که مرتبهٔ HK/H ، m/m_1 را عاد می‌کند. بنابر استقرا، زیرگروه A/H از G/H از مرتبهٔ m/m_1 وجود دارد که شامل HK/H است (که در آن مثل بالا $A < G$). واضح است که K زیرگروهی از A است. چون

$$|A| = |H||A/H| = m_1n_1(m/m_1) = mn_1 < mn,$$

بنابر استقرا، K مشمول زیرگروهی از A (و درنتیجه، از G) از مرتبهٔ m می‌باشد.

حالت ۲. مرتبهٔ هرزیرگروه نرمال‌حقیقی G بر n بخشپذیراست. هرگاه H یک زیرگروه نرمال مینیمال باشد (این نوع گروهها وجود دارند، زیرا G متناهی است)، آنگاه، بنابر لم ۱۳۰۷ (سه)، به‌ازای عدد اولی مانند p، $|H| = p^r$. چون $(m,n) = 1$ و $n||H|$، نتیجه می‌شود که $n = p^r$؛ و درنتیجه، H یک pـزیرگروه زیلوف G است. چون H در G نرمال است، H، pـزیرگروه زیلوف منحصر به فرد G است. این استدلال نشان می‌دهد که H تنها زیرگروه نرمال مینیمال G است (در غیر این صورت، به‌ازای اعداد اول متمایزی چون p,q، $n = p^r$ و $n = q^s$). بخصوص، ***هرزیرگروه نرمال نابدیهی G شامل H است.***

(یک) فرض‌کنیم K زیرگروه‌نرمالی‌از G باشد به‌طوری که K/H زیرگروه نرمال مینیمالی از G/H است (نتیجهٔ I ۱۲۰۵۰)۰ بنابر لم ۱۳۰۷ (سه)، $|K/H| = q^s$ (q اول است، $q \neq p$)؛ درنتیجه، $|K| = p^r q^s$. فرض‌کنیم S یک qـزیرگروه زیلوف K بوده و M نرمال ساز S در G باشد. نشان می‌دهیم که $|M| = m$. چون H در K نرمال است، HS زیرگروهی از K است. واضح است که $H \cap S = \langle e \rangle$؛ درنتیجه،

$$|HS| = |H||S|/|H \cap S| = p^r q^s = |K|,$$

که از آنجا $K = HS$.

چون K در G نرمال‌بوده‌و $S < K$، هر مزدوج S در G در K قرار دارد. وچون S زیرگروه‌زیلوف K است، تمام‌این‌زیرگروهها در K مزدوجند. فرض‌کنیم $N = N_K(S)$. در این صورت، بنابر نتیجهٔ ۴.۴، تعداد مزدوجهای S در G، یعنی c، مساوی $[G : M] = [K : N]$است. چون $S < N < K$، داریم $K > HN > HS = K$؛ درنتیجه، $K = HN$ و

$$c = [G : M] = [K : N] = [HN : N] = [H : H \cap N]$$

(نتیجهٔ I ۹۰۵۰)۰

نشان می‌دهیم $H \cap N = \langle e \rangle$، که ایجاب می‌کند که $c = |H| = p^r$؛ و درنتیجه، $|M| = |G|/[G : M] = mp^r/p^r = m$. برای این منظور ما ابتدا نشان می‌دهیم $H \cap N < C(K)$ و سپس ثابت می‌کنیم $C(K) = \langle e \rangle$.

فرض‌کنیم $x \in H \cap N$ و $k \in K$. چون $K = HS$، داریم $k = hs$ $(h \in H,\ s \in S)$. و چون H آبلی است (لم ۱۳۰۷ (سه)) و $x \in H$، کافی است نشان دهیم $xs = sx$ تا داشته باشیم $xk = kx$ و $x \in C(K)$. اما $(xsx^{-1})s^{-1} \in S$، زیرا $x \in N = N_K(S)$. اما $x(sx^{-1}s^{-1}) \in H$، زیرا $x \in H$ و H در G نرمال است. لذا، $xsx^{-1}s^{-1} \in H \cap S = \langle e \rangle$،

که ایجاب می‌کند $xs = sx$.

بـه آسانی معلـوم می‌شود که $C(K)$ یک زیرگروه مشخص K است. چون K در G نرمال است، $C(K)$ ،بنابرلم ۱۳۰۷ (یک) ، در G نرمال می‌باشد. هرگاه $C(K) \neq \langle e \rangle$ ، آنگاه $C(K)$ لزوما " H را دربردارد. ایـن همراه با $K = HS$ ایجاب می‌کند که S در K نرمال باشد. بنابر لم ۱۳۰۷ (دو) و (یک) ، S در K کاملا " پایاست؛ و درنتیجه، در G نرمال است (زیرا $K \lhd G$) . این ایجاب می‌کند که $H < S$ که تناقض است. از اینرو ، $C(K) = \langle e \rangle$.

(دو) فـرض کنیـم M همانند در (یک) بـوده و B زیرگروه G از مرتبهٔ m باشد. اما $|BK|$ بر $|B| = m$ و $|K| = p^r q^s$ بخشپذیـر اسـت. چـون $(m,p) = 1$ ، $|BK|$ بـر $G/K = BK/K \cong B/B \cap K$ بخشپذیراست. ازاینرو، $G = BK$. درنتیجه، $p^r m = nm = |G|$ (نتیجهٔ I ۹.۵۰) ، که‌ایجاب می‌کند که $|B \cap K| = |B|/|G/K| = q^s$. بنابر قضیهٔ دوم زیلوف ، $B \cap K$ با S در K مزدوج اسـت. بـه علاوه ، $B \cap K$ در B نرمال است (زیرا $K \lhd G$) ؛ و درنتیجه ، B مشمول $N_G(B \cap K)$ می‌بـاشد. تحقیق کنید که زیرگروههای مزدوج نرمال‌سازهای مزدوج دارند. ازاینرو ، $N_G(B \cap K)$ و $N_G(S) = M$ در G مزدوجند. لذا ، $|N_G(B \cap K)| = |M| = m$. اما $|B| = m$. بنـابراین ، $B < N_G(B \cap K)$ ایجاب می‌کند که $B = N_G(B \cap K)$. از اینرو ، B و M مزدوج می‌باشند.

(سه) فرض کنیم $D < G$ ، که در آن $|D| = k$ و $k \mid m$. همچنین ، M (از مرتبهٔ m) و H (از مرتبـهٔ p^r کـه $(p,m) = 1$) همانـنـد در (یـک) بـاشند. در این صورت ، $D \cap H = \langle e \rangle$ و $|DH| = |D||H|/|D \cap H| = kp^r$. همـچنیـن $|G| = mp^r$ ، $M \cap H = \langle e \rangle$ ، و $MH = G$ (زیـرا $|MH| = |M||H|/|M \cap H| = mp^r = |G|$) . از اینرو ، $M(DH) = G$ ؛ و لذا ،

$$|M \cap DH| = |M||DH|/|MDH| = m(kp^r)/mp^r = k.$$

فـرض کنیـم $M^* = M \cap DH$ ؛ پس M^* و D مزدوجند (بنابر (دو) که بر گروه DH اعمال شده است) . به‌ازای $a \in G$ ای ، $aM^*a^{-1} = D$. چون $M^* < M$ ، D مشمول در aMa^{-1} (یک مزدوج M) است؛ و لذا ، زیرگروهی از مرتبهٔ m می‌باشد.

این بخش را بـا بیان حدسی از برنساید[1] که مدتها لاینحل بود خاتمه می‌دهیم :

---

1. Burnside

هر گروه متناهی از مرتبهٔ فرد حلپذیر است. این نتیجهٔ جالب اولین بار توسط دبلیو. فیت[1] و ج. تامپسون[2] [۶] در ۱۹۶۳ ثابت شد.

تمرینات

۱. (آ) A_4 حاصلضرب مستقیم زیرگروههای زیلوف خود نیست، ولی از خاصیت زیر برخوردار است: $mn = 12$ و $(m,n) = 1$ ایجاب می‌کنند که زیرگروهی از مرتبهٔ m وجود داشته باشد.

(ب) S_3 دارای زیرگروههایی از مرتبهٔ 1، 2، 3، و 6 است، ولی حاصلضرب مستقیم زیرگروههای زیلوف خود نیست.

۲. فرض کنید G یک گروه بوده و $a,b \in G$. تعویضگر $aba^{-1}b^{-1} \in G$ را با $[a,b]$ نشان دهید. ثابت کنید به‌ازای هر $a,b,c \in G$، $[ab,c] = a[b,c]a^{-1}[a,c]$.

۳. فرض کنید H و K زیرگروههایی از گروه G بوده، و (H,K) زیرگروهی از G باشد که به وسیلهٔ عناصر $\{hkh^{-1}k^{-1} \mid h \in H, k \in K\}$ تولید می‌شود. نشان دهید که

(آ) (H,K) در $H \vee K$ نرمال است؛

(ب) هرگاه $(H,G') = \langle e \rangle$، آنگاه $(H',G) = \langle e \rangle$؛

(پ) $H \lhd G$ اگر و فقط اگر $(H,G) < H$؛

(ت) فرض کنید $K \lhd G$ و $K < H$. در این صورت، $H/K < C(G/K)$ اگر و فقط اگر $(H,G) < K$.

۴. زنجیر $\gamma_i(G)$ از زیرگروههای گروه G را به صورت زیر تعریف کنید:

$$\gamma_1(G) = G,\ \gamma_2(G) = (G,G),\ \gamma_3(G) = (\gamma_{3-1}(G),G)$$

(ر.ک. تمرین ۳). نشان دهید G پوچ‌توان است اگر و فقط اگر به‌ازای m ی، $\gamma_m(G) = \langle e \rangle$.

۵. هر زیرگروه و هر گروه خارج قسمتی یک گروه پوچ‌توان پوچ‌توان است.

[**راهنمایی.** قضیهٔ ۵.۷ یا تمرین ۴.]

۶. (ویلاند[3]) ثابت کنید گروه متناهی G پوچ‌توان است اگر و فقط اگر هر زیرگروه حقیقی ماکزیمال G نرمال باشد. نتیجه بگیرید که هر زیرگروه حقیقی ماکزیمال

---

1. W. Feit 2. J. Thompson 3. Wielandt

اندیس اول دارد. [**راهنمایی.** اگر P یک p ـ زیرگروه زیلوف G باشد، نشان دهید که هر زیرگروه شامل $N_G(P)$ نرمال‌ساز خودش است؛ ر.ک. قضیهٔ ۱۱۰۵.]

۷. هرگاه N یک زیرگروه نرمال نابدیهی از گروه پوچتوان G باشد، آنگاه $N \cap C(G) \neq \langle e \rangle$.

۸. هرگاه D_n گروه‌دو وجهی با مولدهای a از مرتبهٔ n و b از مرتبهٔ 2 باشد، آنگاه

(آ) $a^2 \in D_n'$؛

(ب) اگر n فرد باشد، $D_n' \cong Z_n$؛

(پ) اگر n زوج باشد، $D_n' \cong Z_m$ که در آن $2m = n$؛

(ت) D_n پوچتوان است اگر و فقط اگر n توانی از 2 باشد.

۹. نشان دهید که زیرگروه تعویضگر S_4 مساوی A_4 است. گروه تعویضگر A_4 چیست؟

۱۰. S_n به‌ازای $n \leq 4$ حلپذیر است، ولی S_3 و S_4 پوچتوان نیستند.

۱۱. گروه حلپذیر متناهی نابدیهی G شامل زیرگروه آبلی نرمال $H \neq \langle e \rangle$ است. هرگاه G حلپذیر نباشد، آنگاه G شامل زیرگروه نرمالی مانند H است که $H' = H$.

۱۲. گروهی مانند G وجود ندارد که $G' = S_4$. [**راهنمایی.** تمرینهای ۹ و ۱۲۰۵ ممکن است یاری‌دهنده باشند.]

۱۳. هرگاه G گروه باشد، آنگاه زیرگروه مشتق i ام $G^{(i)}$ یک زیرگروه کاملا" پایا است؛ درنتیجه، $G^{(i)}$ نرمال می‌باشد.

۱۴. هرگاه $N \lhd G$ و $N \cap G' = \langle e \rangle$، آنگاه $N < C(G)$.

۱۵. هرگاه H زیرگروه حقیقی ماکزیمالی از گروه حلپذیر متناهی G باشد، آنگاه $[G : H]$ یک توان اول می‌باشد.

۱۶. به‌ازای هر گروه G، $C(G)$ مشخص است ولی لزوما" کاملا" پایا نیست.

۱۷. هرگاه G یک p ـ گروه آبلی باشد، آنگاه زیرگروه $G[p]$ (ر.ک. لم ۷۰۲) در G کاملا" پایا می‌باشد.

۱۸. هرگاه G یک گروه پوچتوان متناهی باشد، آنگاه هر زیرگروه نرمال مینیمال از G مشمول $C(G)$ بوده و مرتبهٔ اول خواهد داشت.

۸ سریهای نرمال و زیر نرمال

سودمندی سریهای مرکزی افزایشی و زیرگروههای مشتق یک گروه ما را به بررسی سریهای

دیگری از زیرگروهها ترغیب می‌کند. این کار ذیلاً" انجام شده و مشخصات دیگری از گروههای پوچ‌توان و حلپذیر، و نیز قضیهٔ مشهوری از ژردان[1] ـ هولدر[2]، را به دست می‌آوریم.

تعریف ۱۰۸. یک **سری زیرنرمال** ازگروه G زنجیری مانند

$$G = G_0 > G_1 > \cdots > G_n$$

از زیرگروهها می‌باشد به‌طوری که به‌ازای $0 \leq i < n$ ، G_{i+1} در G_i نرمال است. ***عاملهای*** سری گروههای خارج قسمتی G_i/G_{i+1} می‌باشند. ***طول*** سری تعداد شمولهای اکید (یا تعداد عاملهای غیرهمانی) می‌باشد. یک سری زیرنرمال که در آن به‌ازای هر i ، G_i در G نرمال است را **نرمال** می‌نامیم.[3]

یک سری زیرنرمال لزوماً" نرمال نیست (تمرین I ۱۰۰۵۰).

چندمثال. به‌ازای هرگروه G ، سری مشتق $G > G^{(1)} > \cdots > G^{(n)}$ یک سری نرمال است (ر.ک. تمرین ۱۳۰۷). اگر G پوچ‌توان باشد، سری مرکزی افزایشی $C_1(G) < \cdots < C_n(G) = G$ یک سری نرمال برای G است.

تعریف ۲۰۸. فرض کنیم $G = G_0 > G_1 > \cdots > G_n$ یک سری زیرنرمال باشد. تظریف ***یک مرحله‌ای*** این سری سریی است به شکل

$$G = G_0 > \cdots > G_i > N > G_{i+1} > \cdots > G_n$$

یا

$$G = G_0 > \cdots > G_n > N,$$

که در آن N یک زیرگروه نرمال G_i بوده و (اگر $i < n$) G_{i+1} در N نرمال است. یک **تظریف** سری زیرنرمال S سری زیرنرمالی است که از S با دنباله‌ای متناهی از تظریفهای یک مرحله‌ای به دست آمده باشد. یک تظریف S را **حقیقی** نامیم اگر طولش از طول S

---

1. Jordan
2. Hölder

۳. *بعضی از مولفان به جای "زیرنرمال" "نرمال" به‌کار می‌برند.*

بزرگتر باشد.

تعریف ۳۰۸. سری زیر نرمال $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ یک **سری ترکیبی** است اگر هر عامل G_i/G_{i+1} ساده باشد. اگر هر عامل آبلی باشد، سری زیرنرمال $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ یک **سری حلپذیر** است.

از مطلب زیرمکرر در سریهای ترکیبی استفاده می‌شود: هرگاه N یک زیرگروه نرمال گروه G باشد، آنگاه هر زیر گروه نرمال G/N به شکل H/N است، که در آن H زیرگروه نرمالی از G شامل N می‌باشد (نتیجهٔ I ۱۲۰۵۰). بنابراین، وقتی $N \neq G$، G/N ساده است اگر و فقط اگر N در مجموعهٔ تمام زیرگروههای نرمال M از G با خاصیت $M \neq G$ ماکزیمال باشد (چنین زیرگروه N یک **زیرگروه نرمال ماکزیمال** G نام دارد).

قضیهٔ ۴۰۸. (یک) *هر گروه متناهی G دارای سری ترکیبی است.*
(دو) *هر تظریف یک سری حلپذیر سریی حلپذیر است.*
(سه) *یک سری زیرنرمال سری ترکیبی است اگر و فقط اگر تظریف حقیقی نداشته باشد.*

برهان. (یک) فرض کنیم G_1 زیرگروه نرمال ماکزیمالی از G باشد؛ پس، بنابر نتیجهٔ I ۱۲۰۵۰، G/G_1 ساده است. فرض کنیم G_2 یک زیرگروه نرمال ماکزیمال G_1 باشد، و به همین ترتیب تا آخر. چون G متناهی است، این فرایند باید به $G_n = \langle e \rangle$ ختم شود. لذا، $G > G_1 > \cdots > G_n = \langle e \rangle$ یک سری ترکیبی می‌باشد.
(دو) هرگاه G_i/G_{i+1} آبلی بوده و $G_{i+1} \lhd H \lhd G_i$، آنگاه H/G_{i+1} آبلی است، زیرا زیرگروهی از G_i/G_{i+1} است، و G_i/H نیز آبلی است، زیرا، طبق قضیهٔ سوم یکریختی I ۱۰۵۰، با خارج‌قسمت $(G_i/G_{i+1})/(H/G_{i+1})$ یکریخت است. حال نتیجه فورا" به دست می‌آید.
(سه) هرگاه $G_{i+1} \lneq H \lneq G_i$، آنگاه، بنابر نتیجهٔ I ۱۲۰۵۰، H/G_{i+1} یک زیرگروه نرمال‌حقیقی از G_i/G_{i+1} است و هرزیرگروه نرمال حقیقی G_i/G_{i+1} به این شکل است. حال باتوجه به اینکه سری زیر نرمال $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ تظریف حقیقی دارد اگر و فقط اگر زیرگروهی مانند H موجود باشد به‌طوری که به‌ازای i ی، $G_{i+1} \lneq H \lneq G_i$،

نتیجه به دست خواهد آمد .

قضیهٔ ۵۰۸ . *گروه G حلپذیر است اگر و فقط اگر سری حلپذیر داشته باشد .*

برهان. هرگاه G حلپذیر باشد ، آنگاه ، بنابر قضیهٔ ۸۰۷ ، سری مشتق $G > G^{(1)} > G^{(2)} > \cdots > G^{(n)} = \langle e \rangle$ یک سری حلپذیر است . هرگاه $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ یک سری حلپذیر برای G باشد ، آنگاه ، بنابر قضیهٔ ۸۰۷ ، آبلی بودن G/G_1 ایجاب می‌کند که $G_1 > G^{(1)}$ ؛ نیز آبلی بودن G_1/G_2 ایجاب می‌کند که $G_2 > G_1' > G^{(2)}$. به استقرا ادامه داده نتیجه می‌گیریم که به‌ازای هر i ، $G_i > G^{(i)}$ ؛ بخصوص، $\langle e \rangle = G_n > G^{(n)}$ و G حلپذیر است .

چند مثال. گروه‌دووجهی D_n حلپذیراست ، زیرا $D_n > \langle a \rangle > \langle e \rangle$ یک‌سری‌حلپذیر است ، که در آن a مولد مرتبهٔ n است (درنتیجهٔ ۱۰۴ ، $D_n/\langle a \rangle \cong Z_2$) . به همین نحو ، هرگاه $|G| = pq$ ($p > q$ اولند) ، آنگاه G شامل عنصری‌مانند a از مرتبهٔ p بوده و $\langle a \rangle$ در G نرمال‌است (نتیجهٔ ۱۰۴) . لذا ، $G > \langle a \rangle > \langle e \rangle$ یک‌سری‌حلپذیر بوده و G حلپذیر می‌باشد . به‌طور کلی ، داریم

حکم ۶۰۸ . *گروه متناهی G حلپذیر است اگر و فقط اگر G دارای سری ترکیبی باشدکه عواملش دوری و از مرتبهٔ اول باشند .*

برهان. هر سری (ترکیبی) با عوامل دوری یک سری حلپذیر است . به عکس، فرض کنیم $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ یک سری حلپذیر برای G باشد . اگر $G_0 \neq G_1$ ، H_1 را یک زیرگروه نرمال ماکزیمال $G = G_0$ می‌گیریم که شامل G_1 باشد . اگر $H_1 \neq G_1$ ، H_2 را یک زیرگروه نرمال ماکزیمال H_1 می‌گیریم که شامل G_1 باشد ، و غیره . چون G متناهی است ، این روش سری

$$G > H_1 > H_2 > \cdots > H_k > G_1$$

را می‌دهد که در آن هر زیرگروه یک زیرگروه نرمال ماکزیمال قبلی خود است ؛ و لذا ، هر عامل‌ساده می‌باشد . بنابر قضیهٔ ۴۰۸ (دو) ، با انجام این در مورد هر جفت (G_i, G_{i+1})

تظریف حلپذیری مانند $G = N_0 > N_1 > \cdots > N_r = \langle e \rangle$ از سری اصلی به دست می‌آید. هر عامل این سری آبلی و ساده است؛ و درنتیجه، دوری از مرتبهٔ اول است (تمرین I ۳۰۴۰). بنابراین، $G > N_1 > \cdots > N_r = \langle e \rangle$ یک سری ترکیبی می‌باشد.

یک گروه ممکن است سری زیرنرمال یا حلپذیر بسیار داشته باشد. همچنین، ممکن است چندسری ترکیبی متفاوت داشته باشد (تمرین ۱). با اینحال، اینک نشان می‌دهیم که هر دو سری ترکیبی یک گروه به معنی زیر معادلند.

تعریف ۷۰۸. دو سری زیرنرمال S و T ازگروه G **معادل**اند اگر تناظر یک به یکی بین عوامل نابدیهی S و عوامل نابدیهی T موجود باشد به‌طوری که عاملهای نظیر گروههایی یکریخت باشند.

برای معادل بودن دو سری زیرنرمال لازم نیست تعداد جملات هر دو مساوی باشند، ولی باید طولهایشان یکسان باشد (یعنی، یک تعداد عامل نابدیهی داشته باشند). واضح است که معادل بودن سریهای زیرنرمال یک رابطهٔ هم‌ارزی است.

لم ۸۰۸. هرگاه S یک سری ترکیبی از گروه G باشد، آنگاه هر تظریف S با S معادل است.

برهان. فرض کنیم S با $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ نموده‌شده باشد. بنابر قضیهٔ ۴۰۸ (سه)، S تظریف حقیقی ندارد. این ایجاب می‌کند که تظریفهای S فقط با درج نسخه‌های اضافی از هر G_i به دست می‌آیند. درنتیجه، تعداد عوامل نابدیهی هر تظریف S درست‌مساوی تعداد عوامل نابدیهی S است؛ و لذا، با S معادل می‌باشد.

لم زیر کاملا" تکنیکی است. ارزش آن در برهان ۱۰۸ بلافاصله معلوم می‌شود.

لم ۹۰۸ (زاسن هاوس[1]). فرض کنیم A^*, A, B^*, B زیرگروههایی از گروه G باشند

---

1. *Zassenhaus*

به‌طوری که A^* در A و B^* در B نرمال است.

(یک) $A^*(A \cap B^*)$ **زیرگروه نرمالی از** $A^*(A \cap B)$ **است؛**

(دو) $B^*(A^* \cap B)$ **زیرگروه نرمالی از** $B^*(A \cap B)$ **است؛**

(سه) $A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(A \cap B)/B^*(A^* \cap B)$.

برهان. چون B^* در B نرمال است، $A \cap B^* = (A \cap B) \cap B^*$ زیرگروه نرمالی از $A \cap B$ است (قضیهٔ I ۳.۵۰ (یک))؛ به همین نحو، $A^* \cap B$ در $A \cap B$ نرمال می‌باشد. درنتیجه، $D = (A^* \cap B)(A \cap B^*)$ زیرگروه نرمالی از $A \cap B$ است (قضیهٔ I ۳.۵۰ (سه) و تمرین I ۱۳.۵۰). قضیهٔ I ۳.۵۰ (سه) نیز ایجاب می‌کند که $A^*(A \cap B)$ و $B^*(A \cap B)$ به ترتیب زیرگروههایی از A و B اند. بروریختی $f : A^*(A \cap B) \to (A \cap B)/D$ با هستهٔ $A^*(A \cap B^*)$ را تعریف می‌کنیم. این ایجاب می‌کند که $A^*(A \cap B^*)$ در $A^*(A \cap B)$ نرمال باشد (قضیهٔ I ۵.۵۰) و

$$A^*(A \cap B)/A^*(A \cap B^*) \cong (A \cap B)/D$$ (نتیجهٔ I ۷.۵۰)

$f : A^*(A \cap B) \to (A \cap B)/D$ را به‌صورت‌زیر تعریف می‌کنیم. اگر $a \in A^*$، $c \in A \cap B$ قرارمی‌دهیم $f(ac) = Dc$. f تعریف‌شده‌است، زیرا $ac = a_1c_1$ $(a,a_1 \in A^*;\ c,c_1 \in A \cap B)$ ایجاب می‌کند که

$$c_1c^{-1} = a_1^{-1}a \in (A \cap B) \cap A^* = A^* \cap B < D$$

که از آنجا $Dc_1 = Dc$. واضح است که f سورژکتیو است. f بروریختی است، زیرا

$$f[(a_1c_1)(a_2c_2)] = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)\,f(a_2c_2)$$

که در آن $a_i \in A^*, c_j \in A \cap B$، و $c_1a_2 = a_3c_1$، زیرا A^* در A نرمال است. بالاخره، $ac \in \operatorname{Ker} f$ اگروفقط اگر $c \in D$؛ یعنی، اگر و فقط اگر $c = a_1c_1$، که در آن $a_1 \in A^* \cap B$ و $c_1 \in A \cap B^*$. از اینرو، $ac \in \operatorname{Ker} f$ اگروفقط اگر $ac = (aa_1)c_1 \in A^*(A \cap B^*)$. بنابراین، $\operatorname{Ker} f = A^*(A \cap B^*)$.

استدلالی متقارن نشان می‌دهد که $B^*(A \cap B)$ در $B^*(A^* \cap B)$ نرمال است و $B^*(A \cap B)/B^*(A^* \cap B) \cong (A \cap B)/D$، که از آن (سه) فوراً نتیجه می‌شود.

قضیهٔ ۱۰.۸ (شریر[1]). هر دو سری زیرنرمال [نرمال] گروه G تظریفهای زیرنرمال

---

1. *Schreier*

[نرمال] دارند که با هم معادلند .

برهان . فرض کنیم $G = G_0 > G_1 > \cdots > G_n$ و $G = H_0 > H_1 > \cdots > H_m$ سریهایی زیرنرمال [نرمال] باشند . همچنین $G_{n+1} = \langle e \rangle = H_{m+1}$ ، و بهازای هر $0 \leq i \leq n$ ، گروههای زیر را درنظر میگیریم :

$$G_i = G_{i+1}(G_i \cap H_0) > G_{i+1}(G_i \cap H_1) > \cdots > G_{i+1}(G_i \cap H_j) > G_{i+1}(G_i \cap H_{j+1}) > \cdots > G_{i+1}(G_i \cap H_m) > G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}.$$

بهازای هر $0 \leq j \leq m$ ، لم زاسن هاوس (اعمال شده بر G_i ، G_{i+1} ، H_{j+1} ، H_j و) نشان میدهد که $G_{i+1}(G_i \cap H_{j+1})$ در $G_{i+1}(G_i \cap H_j)$ نرمال است . [هرگاه سریهای اصلی هر دو نرمال باشند ، آنگاه ، طبق قضیهٔ I ۳۰۵۰ (سه) و تمرینهای I ۲۰۵۰ و I ۱۳۰۵۰ ، هر $G_{i+1}(G_i \cap H_j)$ در G نرمال است .] لذا ، با درج این گروهها بین هر G_i و G_{i+1} و نمایش $G_{i+1}(G_i \cap H_j)$ به وسیلهٔ $G(i,j)$ ، تظریف زیر نرمال [نرمال] زیر از سری $G = G_0 > G_1 > \cdots > G_n$ بهدست میآید :

$$G = G(0,0) > G(0,1) > \cdots > G(0,m) > G(1,0) > G(1,1) > G(1,2) > \cdots > G(1,m) > G(2,0) > \cdots > G(n-1,m) > G(n,0) > \cdots > G(n,m),$$

که در آن $G(i,0) = G_i$. توجه کنید که این تظریف $(n+1)(m+1)$ جمله (نه لزوما " متمایز) دارد . استدلالی متقارن نشان میدهدکه تظریف زیر از $G = H_0 > H_1 > \cdots > H_m$ (که در آن $H(i,j) = H_{j+1}(G_i \cap H_j)$ و $H(0,j) = H_j$) وجود دارد :

$$G = H(0,0) > H(1,0) > \cdots > H(n,0) > H(0,1) > H(1,1) > H(2,1) > \cdots > H(n,1) > H(0,2) > \cdots > H(n,m-1) > H(0,m) > \cdots > H(n,m).$$

این تظریف نیز دارای $(n+1)(m+1)$ جمله میباشد . بنابر لم زاسن هاوس ۹۰۸ (اعمال شده بر G_{i+1} ، G_i ، H_{j+1} ، و H_j) ، بهازای هر جفت (i,j) $(0 \leq i \leq n,\ 0 \leq j \leq m)$ یک یکریختی وجود دارد :

$$\frac{G(i,j)}{G(i,j+1)} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)} = \frac{H(i,j)}{H(i+1,j)}.$$

این تناظر یک به یک مطلوب بین عاملها را به دست داده و نشان میدهد که تظریفها معادل میباشند .

قضیهٔ ۱۱.۸ (ژردان ــ هولدر). *هر دو سری ترکیبی گروه G معادلند. بنابراین، هر گروهی که سری ترکیبی داشته باشد لیست منحصربه فردی از گروههای ساده را معین می‌کند.*

تبصره. قضیه از وجود سریی ترکیبی برای یک گروه داده شده سخن **نمی‌گوید**.

برهان ۱۱.۸. چون سریهای ترکیبی سریهایی زیرنرمال‌اند، بنابر قضیهٔ ۱۰.۸، هر دو سری ترکیبی تظریفهای معادلی دارند. اما، طبق لم ۸.۸، هر تظریف سری ترکیبی S با S معادل است. پس نتیجه می‌شود که هر دو سری ترکیبی معادل می‌باشند.

قضیهٔ ژردان ــ هولدر بیانگر این است که اطلاعاتی از گروههای ساده ممکن است مفید باشد. کار بزرگی که در سنوات اخیر شده است رده‌بندی کامل تمام گروههای سادهٔ متناهی است. این نتیجهٔ قابل توجه مبتنی بر کارهای تعداد زیادی متخصص در نظریهٔ گروههاست. برای آشنایی با مسئله و خلاصه‌ای از روش اثبات، ر.ک. کتاب **گروههای سادهٔ متناهی** از دانیل گورن اشتاین[1]. گروههای سادهٔ غیرآبلی از مرتبهٔ کوچک بسیار نادرند. می‌توان ثابت کرد که (با تقریب یکریختی) تنها دو گروه سادهٔ غیرآبلی از مرتبهٔ کوچکتر از 200، یعنی A_5 و زیرگروهی از S_7 از مرتبهٔ 168، وجود دارند (ر.ک. تمرینهای ۱۳ تا ۲۰).

تمرینات

۱. (آ) یک سری نرمال از D_4 بیابید که از 4 زیرگروه تشکیل شده باشد.
(ب) تمام سریهای ترکیبی گروه D_4 را بیابید.
(پ) قسمت (ب) را برای گروه A_4 حل کنید.
(ت) قسمت (ب) را برای گروه $S_3 \times Z_2$ حل کنید.
(ث) تمام عوامل ترکیبی S_4 و D_6 را بیابید.

۲. هرگاه $G = G_0 > G_1 > \cdots > G_n$ یک سری‌زیرنرمال از گروه متناهی G باشد، آنگاه $|G| = \left(\prod_{i=0}^{n-1} |G_i/G_{i+1}|\right)|G_n|$.

---

1. Daniel Gorenstein *Finite Simple Groups* (Plenum Publishing Corp., 1982).

۳ . هرگاه N زیرگروه نرمال ساده‌ای از گروه G بوده و G/N سری ترکیبی داشته باشد ، آنگاه G نیز سری ترکیبی دارد .

۴ . سری ترکیبی یک گروه یک سری زیرنرمال با طول ماکزیمال (متناهی) می‌باشد .

۵ . یک گروه آبلی سری ترکیبی دارد اگر و فقط اگر متناهی باشد .

۶ . هرگاه $H \lhd G$ ، که در آن G سری ترکیبی دارد ، آنگاه G سریی ترکیبی دارد که یکی از جملاتش H است .

۷ . هر گروه حلپذیر دارای سری ترکیبی متناهی است .

۸ . هرگاه H و K زیرگروههای حلپذیری از G باشندو $H \lhd G$ ، آنگاه HK یک زیرگروه حلپذیر G است .

۹ . هر گروه از مرتبهٔ $p^a q^b$ (p,q اول) حلپذیر است .

۱۰ . گروه G پوچتوان است اگر و فقط اگر یک سری نرمال مانند $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ وجود داشته باشد بطوری که بازای هر i ، $G_i/G_{i+1} < C(G/G_{i+1})$.

۱۱ . (آ) نشان دهید که شبیه قضیهٔ ۱۱.۷ برای گروههای پوچتوان نادرست است [S_3 را درنظر بگیرید] .

(ب) هرگاه $H < C(G)$ و G/H پوچتوان باشد ، آنگاه G پوچتوان است .

۱۲ . با اعمال قضیهٔ ژردان ـ هولدر بر گروه Z_n ، قضیهٔ اساسی حساب (آشنایی ، قضیهٔ ۷.۶) را ثابت نمایید .

۱۳ . هرگروه‌سادهٔ G از مرتبهٔ 60 با A_5 یکریخت است . [**راهنمایی .** از نتیجهٔ ۹.۴ استفاده کنید : هرگاه $H < G$ ، آنگاه $[G:H] \geq 5$.(زیرا بازای $n \leq 4$ ، $|S_n| < 60$) ؛ هرگاه $[G:H] = 5$ ، آنگاه ، طبق قضیهٔ ۸.۶.۱ ، $G \cong A_5$. این فرض که زیرگروهی با اندیس 5 وجود ندارد به تناقض منجر می‌شود .]

۱۴ . گروه سادهٔ غیرآبلی از مرتبهٔ کوچکتر از 60 وجود ندارد .

۱۵ . فرض کنید G زیرگروهی از S_7 باشد که به وسیلهٔ (1234567) و (34)(26) تولید شده است . نشان دهید که $|G| = 168$.

در تمرینهای ۱۶ تا ۲۰ بطور خلاصه ثابت می‌شود که گروه G تمرین ۱۵ ساده است . ما ، همانند در اولین مثال پس از تعریف ۱۰.۴ ، فرض می‌کنیم G بر مجموعهٔ $S = \{1,2,3,4,5,6,7\}$ عمل کند و از تمرین ۶.۴ استفاده می‌کنیم .

۱۶ . گروه G متعدی است (ر.ک. تمرین ۶.۴) .

۱۷ . به‌ازای هر $x \in S$ ، G_x یک‌زیرگروه (حقیقی) ماکزیمال از G است . اثبات این امر در چند مرحله صورت می‌گیرد :

(آ) یک **بلوک** از G زیرمجموعه‌ای‌مانند T از S است‌به‌طوری‌که‌به‌ازای‌هر $g \in G$ ، $gT = T$ یا $gT \cap T = \varnothing$ ، که در آن $gT = \{gx \mid x \in T\}$. نشان دهید هرگاه T یک بلوک باشد ، آنگاه $|T|$ ، 7 را عاد می‌کند .

[**راهنمایی .** فرض کنید $H = \{g \in G \mid gT = T\}$ و نشان دهید به‌ازای $x \in T$ ، $G_x < H$ و $[H : G_x] = |T|$. ازاینرو ، $|T|$ ، $[G : G_x] = [G : H][H : G_x]$ را عاد می‌کند . اما ، بنابر تمرین ۶.۴ (آ) و قضیهٔ ۳.۴ ، $[G : G_x] = 7$.]

(ب) هرگاه G_x ماکزیمال نباشد ، آنگاه بلوکی مانند T از G وجود دارد به‌طوری که $|T| \neq 7$ ، که با قسمت (آ) متناقض است .

[**راهنمایی .** اگر $G_x \leq H < G$ ، نشان دهید که H بر S متعدی نیست (زیرا $1 \leq [H : G_x] < |S|$ ، که با تمرین ۶.۴ (ت) متناقض است) . فرض کنید $T = \{hx \mid h \in H\}$. چون H متعدی نیست ، $|T| < |S|$ و چون $H \neq G_x$ ، داریم $|T| > 1$. نشان دهید که T یک بلوک است .]

۱۸ . هرگاه $N \lhd G \neq (1)$ ، آنگاه $|N|$ را 7 عاد می‌کند . [**راهنمایی .** تمرین ۶.۴ (پ) ایجاب می‌کند که به‌ازای هر $x \in S$ ، $G_x \leq NG_x$ و این ، بنابر تمرین ۱۷ ، ایجاب می‌کند که به‌ازای هر $x \in S$ ، $NG_x = G$ و این ، ایجاب می‌کند که N بر S متعدی است و این ، بنابر تمرین ۶.۴ (ت) ، ایجاب می‌کند که $|N|$ ، 7 را عاد خواهد کرد .

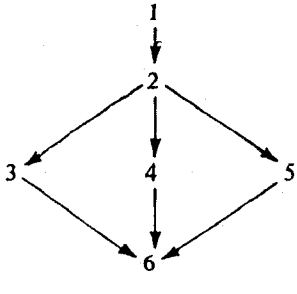
۱۹ . گروه G شامل زیرگروهی مانند P از مرتبهٔ 7 است به طوری که کوچکترین زیرگروه نرمال G شامل P خود G است .

۲۰ . هرگاه $N \lhd G \neq (1)$ ، آنگاه $N = G$ ؛ از اینرو ، G ساده است . [با استفاده از تمرین I ۱۹.۵۰ و تمرین ۱۸ ، نشان‌دهید که $P < N$ ؛ تمرین ۱۹ را به کار برید .]

۳

حلقه‌ها

مفهوم اساسی دیگر در جبر مفهوم حلقه است. مسئلهٔ رده‌بندی تمام حلقه‌ها (در یک رده) با تقریب یکریختی از مسئلهٔ نظیر در مورد گروهها خیلی مشکلتر است. این مسئله تا حدودی در فصل نه مورد بحث قرار می‌گیرد. قسمت اعظم فصل حاضر به ارائهٔ مطالبی از نظریهٔ حلقه‌ها اختصاص دارد که در چند حیطه از جبر بیشترین کاربرد را دارند. در دو بخش اول حلقه‌ها، همریختیها، و ایده‌آلها را بررسی می‌کنیم. بسیاری از (اما نه همهٔ) این مطالب تعمیم سرراست مفاهیمی به حلقه‌ها هستند که سودمندی آنها در نظریهٔ گروهها ثابت شده است. بخشهای ۳ و ۴ به حلقه‌های تعویضپذیری اختصاص دارند که از بسیاری جهات شبیه به حلقهٔ اعداد صحیح می‌باشند. بخشپذیری، تجزیه، حلقه‌های اقلیدسی، دامنه‌های ایده‌آل اصلی، و یکتایی تجزیه در بخش ۳ بررسی می‌شوند. در بخش ۴، ساخت آشنای میدان اعداد گویا از حلقهٔ اعداد صحیح تعمیم یافته و حلقه‌های خارج قسمتی یک حلقهٔ تعویضپذیر دلخواه به تفصیل مطرح می‌شوند. در دو بخش آخر، حلقهٔ چند جمله‌ایها از n مجهول روی حلقهٔ R مطالعه می‌شود. بخصوص، مفاهیم بخش ۳ در حلقه‌های چند جمله‌ای مطالعه خواهند شد (بخش ۶). ارتباط تقریبی بخشهای این فصل به صورت زیر است:



بخش ۶ فقط به قسمتهایی از بخشهای ۴ و ۵ نیاز دارد.

۱ حلقه‌ها و همریختیها

مفاهیم اساسی نظریهٔ حلقه‌ها را تعریف و مثالهای متعددی می‌آوریم. چند مطلب محاسباتی که مکرر به کار می‌روند نیز عرضه می‌شود. تنها مشکل در باب آنها وجود اصطلاحات زیادی است که باید در زمانی کوتاه هضم شوند.

تعریف ۱.۱. یک **حلقه** مجموعه‌ای است ناتهی مانند R همراه با دو عمل دوتایی (که معمولاً به صورت جمع $(+)$ و ضرب نموده می‌شوند) به‌طوری‌که

(یک) $(R,+)$ یک گروه آبلی است؛

(دو) به‌ازای هر $a,b,c \in R$، $(ab)c = a(bc)$ (ضرب شرکتپذیر است)؛

(سه) $a(b+c) = ab + ac$ و $(a+b)c = ac + bc$ (قوانین پخشپذیری از چپ و از راست).

هرگاه، علاوه بر این،

(چهار) به‌ازای هر $a,b \in R$، $ab = ba$،

آنگاه گوییم R یک **حلقهٔ تعویضپذیر** است. هرگاه R شامل عنصری مانند 1_R باشد به طوری‌که

(پنج) به‌ازای هر $a \in R$، $1_R a = a 1_R = a$،

آنگاه گوییم R یک **حلقهٔ یکدار**[1] است.

تبصره. برای نمایش نگاشت همانی $R \to R$ از علامت 1_R نیز استفاده می‌شود. این علامت ابهامی ایجاد نمی‌کند.

عنصر همانی جمعی یک حلقه **عنصر صفر** نام دارد و با 0 نموده می‌شود. هرگاه R یک حلقه بوده، و $a \in R$ و $n \in \mathbf{Z}$، آنگاه na معنی معمول خود برای گروههای جمعی را دارد (تعریف I ۸.۱۰)؛ مثلاً، وقتی $n > 0$، $na = a + a + \cdots + a$ (n جمعوند).

---

[1] حلقهٔ یکدار R را حلقه با واحد نیز می‌نامند و 1_R را واحد حلقه گویند. م.

پیش از ذکر چند مثال از حلقه‌ها ، قضیهٔ زیر را می‌آوریم .

قضیهٔ ۲.۱ . فرض کنیم R یک حلقه باشد . در این صورت ،

(یک) به‌ازای هر $a \in R$ ، $0a = a0 = 0$ ؛

(دو) به‌ازای هر $a,b \in R$ ، $(-a)b = a(-b) = -(ab)$ ؛

(سه) به‌ازای هر $a,b \in R$ ، $(-a)(-b) = ab$ ؛

(چهار) به‌ازای هر $n \in \mathbf{Z}$ **و هر** $a,b \in R$ ، $(na)b = a(nb) = n(ab)$ ؛

(پنج) به‌ازای هر $a_i,b_j \in R$ ، $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

طرح برهان . (یک) $0a = (0+0)a = 0a + 0a$ ، که از آنجا $0a = 0$.
(دو) $ab + (-a)b = (a + (-a))b = 0b = 0$ ، که از آنجا ، بنابر قضیهٔ I ۲.۱۰ (سه) ، $(-a)b = -(ab)$. قسمت (دو) قسمت (سه) را ایجاب می‌کند . قسمت (پنج) به استقرا ثابت می‌شود و قسمت (چهار) حالت خاصی از قسمت (پنج) است .

دردو تعریف‌زیرچند اصطلاح دیگر معرفی می‌شوند ؛ پس از آنها چند مثال خواهیم آورد .

تعریف ۳.۱ . عنصرناصفر a در حلقهٔ R را یک **مقسوم‌علیه صفر چپ** [راست] گوییم اگر عنصرناصفری‌مانند $b \in R$ موجودباشد به‌طوری‌که $ab = 0$ [$ba = 0$] . **مقسوم‌علیه صفر** عنصری از R است که هم مقسوم‌علیه صفر چپ باشد هم مقسوم‌علیه صفر راست .

به‌آسانی معلوم می‌شود که حلقهٔ R مقسوم‌علیه صفر ندارد اگر و فقط‌اگر قوانین حذف از راست و از چپ در R برقرار باشند ؛ یعنی ، به‌ازای هر $a,b,c \in R$ که $a \neq 0$ ،

$$ba = ca \quad \text{یا} \quad ab = ac \quad \Rightarrow \quad b = c.$$

تعریف ۴.۱ . عنصر a در حلقهٔ یکدار R را **معکوسپذیر چپ** [راست] گوییم اگر $c \in R$ ای [$b \in R$ ای] وجودداشته‌باشدکه $ca = 1_R$ [$ab = 1_R$] . عنصر c [b]

معکوس چپ [راست] a نامیده می‌شود. عنصر $a \in R$ که معکوسپذیر چپ و راست باشد **معکوسپذیر** یا **یکه** نامیده می‌شود.

چند تبصره. (یک) معکوسهای چپ و راست یکهٔ a در حلقهٔ یکدار R لزوماً یکی هستند (زیرا $ab = 1_R = ca$ ایجاب می‌کند که $b = 1_R b = (ca)b = c(ab) = c1_R = c$). (دو) مجموعهٔ یکه‌ها در حلقهٔ یکدار R تحت ضرب تشکیل یک گروه می‌دهد.

تعریف ۵۰۱. حلقهٔ تعویضپذیر و یکدار R با خاصیت $1_R \neq 0$ و فاقد مقسوم‌علیه‌های صفر یک ***دامنهٔ صحیح*** نامیده می‌شود. حلقهٔ یکدار D با خاصیت $1_D \neq 0$ که در آن هر عنصر ناصفر یکه باشد یک ***حلقهٔ بخشی*** نام دارد. هر ***میدان*** یک حلقهٔ بخشی تعویضپذیر است.

چند تبصره. (یک) هر دامنهٔ صحیح و هر حلقهٔ بخشی دست‌کم دو عنصر دارد (یعنی، 0 و 1_R). (دو) حلقهٔ یکدار R یک حلقهٔ بخشی است اگر و فقط اگر عناصر ناصفر R تحت ضرب گروه تشکیل دهند (ر.ک. تبصرهٔ (دو) بعد از تعریف ۴۰۱).
(سه) هر میدان F یک دامنهٔ صحیح است، زیرا $ab = 0$ و $a \neq 0$ ایجاب می‌کنند که $b = 1_F b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

چند مثال. حلقهٔ $\mathbf{Z}$ اعداد صحیح یک دامنهٔ صحیح است. مجموعهٔ E مرکب از اعداد صحیح زوج یک حلقهٔ تعویضپذیر بدون واحد است. $\mathbf{Q}$ (اعداد گویا)، $\mathbf{R}$ (اعداد حقیقی)، و $\mathbf{C}$ (اعداد مختلط) همه تحت اعمال معمولی جمع و ضرب میدان هستند. ماتریسهای $n \times n$ روی $\mathbf{Q}$ (یا $\mathbf{R}$ یا $\mathbf{C}$) یک حلقهٔ یکدار تعویض‌ناپذیر تشکیل می‌دهند. در این حلقه، یکه‌ها دقیقاً ماتریسهای نامنفردند.

مثال. به‌ازای هر عدد صحیح و مثبت n، مجموعهٔ Z_n از اعداد صحیح به پیمانهٔ n یک حلقه است. برای جزئیات امر، ر.ک. مثال بعد از قضیهٔ ۵۰۱۰۱. هرگاه n اول نباشد، مثلاً $n = kr$ که در آن $k > 1, r > 1$، آنگاه در Z_n داریم $\bar{k} \neq \bar{0}$، $\bar{r} \neq 0$، و $\bar{k}\bar{r} = \overline{kr} = \bar{n} = \bar{0}$ و درنتیجه $\bar{k}$ و $\bar{r}$ مقسوم‌علیه‌های صفرند. هرگاه p اول

باشد، آنگاه، بنابر تمرین ۷.۱۰.۱، Z_p یک میدان است.

مثال. فرض کنیم A گروهی آبلی بوده و $\mathrm{End}\ A$ مجموعهٔ درونریختیهای $f: A \to A$ باشد. در $\mathrm{End}\ A$ جمع را با $(f+g)(a) = f(a) + g(a)$ تعریف می‌کنیم. تحقیق کنید که $f+g \in \mathrm{End}\ A$. چون A آبلی است، تحت این جمع $\mathrm{End}\ A$ یک گروه آبلی می‌شود. عمل ضرب در $\mathrm{End}\ A$ را ترکیب توابع اختیار می‌کنیم. در این صورت، $\mathrm{End}\ A$ یک حلقهٔ (احتمالاً " تعویض‌ناپذیر) یکدار با واحد $1_A : A \to A$ است.

مثال. فرض کنیم G یک‌گروه (ضربی) و R یک حلقه باشد. همچنین، $R(G)$ گروه آبلی جمعی $\sum_{g \in G} R$ (یک نسخه از R به‌ازای هر $g \in G$) باشد. شایسته است برای عناصر $R(G)$ نمادهای جدیدی اختیار شود. یک عنصر $x = \{r_g\}_{g \in G}$ از $R(G)$ فقط تعدادی متناهی مختص ناصفر دارد؛ مثلاً "، $r_{g_1}, \ldots, r_{g_n}$ $(g_i \in G)$. x را با **مجموع صوری** $r_{g_1}g_1 + r_{g_2}g_2 + \cdots + r_{g_n}g_n$ یا $\sum_{i=1}^{n} r_{g_i}g_i$ نشان می‌دهیم. همچنین، صفر بودن بعضی از r_{g_i} ها یا تکرار برخی g_i ها را مجاز می‌دانیم؛ درنتیجه، یک عنصر از $R(G)$ را می‌توان به‌طور صوری به‌طرق مختلف نوشت (مثلاً "، $r_1g_1 + 0g_2 = r_1g_1$ یا $r_1g_1 + s_1g_1 = (r_1 + s_1)g_1$). با این نمادها، جمع در گروه $R(G)$ با رابطهٔ زیر داده می‌شود:

$$\sum_{i=1}^{n} r_{g_i}g_i + \sum_{i=1}^{n} s_{g_i}g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i})g_i;$$

(با درج ضرایب صفر در صورت لزوم می‌توان همیشه فرض کرد که دو مجموع صوری دارای اندیسهای $g_1, \ldots, g_n$ یکسان‌هستند). ضرب در $R(G)$ را به صورت زیر تعریف می‌کنیم:

$$\left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{j=1}^{m} s_j h_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} (r_i s_j)(g_i h_j);$$

این دارای معنی‌است، زیرا در هر دوی R $(r_i s_j)$ و G $(g_i h_j)$ ضرب تعریف شده است؛ و لذا، عبارت سمت راست یک مجموع صوری طبق مطلوب است. $R(G)$ با این اعمال یک حلقه است؛ آنرا **حلقهٔ گروهی** G روی R می‌نامند. $R(G)$ تعویضپذیر است اگر و فقط اگر هر دوی R و G تعویضپذیر باشند. هرگاه R دارای واحد 1_R بوده، و e عنصر همانی G

باشد، آنگاه $1_R e$ عنصر واحد $R(G)$ می‌باشد.

مثال. فرض کنیم $\mathbf{R}$ میدان اعداد حقیقی و S مجموعهٔ علایم $1,i,j,k$ باشد. همچنین، K گروه آبلی جمعی $\mathbf{R}\oplus\mathbf{R}\oplus\mathbf{R}\oplus\mathbf{R}$ بوده و عناصر K را به صورت مجموعهای صوری $(a_0,a_1,a_2,a_3) = a_0 1 + a_1 i + a_2 j + a_3 k$ می‌نویسیم. در این صورت، $a_0 1 + a_1 i + a_2 j + a_3 k = b_0 1 + b_1 i + b_2 j + b_3 k$ اگر و فقط اگر به‌ازای هر i، $a_i = b_i$. این قراردادها را می‌پذیریم که $a_0 1 \in K$ را با $a_0 \in \mathbf{R}$ یکی گرفته و جملات با ضرایب صفر را می‌توان حذف کرد (مثلاً "$4 + 2j = 4\cdot 1 + 0i + 2j + 0k$ و $i = 0 + 1i + 0j + 0k$"). در این صورت، جمع در K به صورت زیر تعریف می‌شود:

$$\begin{aligned}&(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)\\ &= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k.\end{aligned}$$

و ضرب در K به صورت زیر تعریف می‌گردد:

$$\begin{aligned}&(a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k)\\ &= (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i\\ &\quad + (a_0 b_2 + a_2 b_0 + a_3 b_1 - a_1 b_3)j + (a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1)k.\end{aligned}$$

این فرمول ضرب از ضرب جمله به جملهٔ مجموعهای صوری با درنظر گرفتن روابط زیر به دست آمده است: (یک) شرکتپذیری؛ (دو) $ri = ir;\ rj = jr,\ rk = kr$ (به‌ازای هر $r \in \mathbf{R}$)؛ (سه) $i^2 = j^2 = k^2 = ijk = -1;\ ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j$. تحت این ضرب یک حلقهٔ بخشی تعویض‌ناپذیر است که در آن معکوس ضربی $a_0 + a_1 i + a_2 j + a_3 k$ عبارت است از $(a_0/d) - (a_1/d)i - (a_2/d)j - (a_3/d)k$، که در آن $d = a_0^2 + a_1^2 + a_2^2 + a_3^2$. K حلقهٔ بخشی **چهارتاهای حقیقی** نام دارد. چهارتاها را می‌توان زیر حلقه‌ای از حلقهٔ تمام ماتریسهای 2×2 روی میدان $\mathbf{C}$ اعداد مختلط تعبیر کرد (تمرین ۸).

تعریف ۱۰۱ نشان می‌دهد که عناصر حلقهٔ R تحت ضرب یک نیمگروه (تکگون اگر R دارای واحد باشد) تشکیل می‌دهند. درنتیجه، تعریف I ۸۰۱۰ قابل اعمال بوده و نماگیری در R تعریف شده است. به‌ازای هر $a \in R$ و $n \in \mathbf{N}^*$، داریم $a^n = a\cdots a$ (n عامل) و، اگر R دارای واحد باشد، $a^0 = 1_R$. بنابر قضیهٔ I ۹۰۱۰،

$$a^m a^n = a^{m+n} \quad \text{و} \quad (a^m)^n = a^{mn}$$

تفریق در حلقهٔ R به‌طور معمول تعریف می‌شود: $a - b = a + (-b)$. واضح است که به‌ازای هر $a,b,c \in R$، $a(b-c) = ab - ac$ و $(a-b)c = ac - bc$.

قضیهٔ بعد در محاسبات بسیار مفید است. به یاد آورید که هرگاه k و n اعدادی صحیح باشند که $0 \le k \le n$، آنگاه **ضریب دوجمله‌ای** $\binom{n}{k}$ عدد $n!/(n-k)!k!$ است، که در آن $0! = 1$ و، به‌ازای $n \ge 1$، $n! = n(n-1)(n-2)\cdots 2\cdot 1$. $\binom{n}{k}$ درواقع یک عدد صحیح است (تمرین ۱۰).

قضیهٔ ۶.۱ (قضیهٔ دوجمله‌ای). *فرض کنیم R حلقه‌ای یکدار بوده، n یک عدد صحیح مثبت باشد، و $a,b,a_1,a_2,\ldots,a_s \in R$.*

(یک) هرگاه $ab = ba$، آنگاه

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k};$$

(دو) هرگاه به‌ازای هر i و j، $a_i a_j = a_j a_i$، آنگاه

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{(i_1!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s},$$

که در آن مجموع روی تمام s تاییهای $(i_1,i_2,\ldots,i_s)$ که $i_1 + i_2 + \cdots + i_s = n$ گرفته شده است.

طرح برهان. (یک) از استقرا بر n و این امر که به‌ازای $k < n$،

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

استفاده کنید (تمرین ۱۰ (پ))؛ قانون پخشپذیری و تعویضپذیری a و b لازمند.

(دو) از استقرا بر s استفاده کنید. حالت $s = 2$ همان قسمت (یک) است، زیرا

$$(a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k} = \sum_{k+j=n} \frac{n!}{k!j!} a_1^k a_2^j.$$

اگر قضیه به‌ازای s درست باشد، ملاحظه می‌شود که بنابر قسمت (یک)

$$(a_1 + \cdots + a_s + a_{s+1})^n = ((a_1 + \cdots + a_s) + a_{s+1})^n = \sum_{k=0}^{n} \binom{n}{k} (a_1 + \cdots + a_s)^k a_{s+1}^{n-k}$$

$$= \sum_{k+j=n} \frac{n!}{k!j!} (a_1 + \cdots + a_s)^k a_{s+1}^j$$

فرض استقرا را به کار برده و محاسبه نمایید .

تعریف ۷.۱ . فرض کنیم R و S حلقه باشند . تابع $f : R \to S$ یک ***همریختی حلقه‌ها*** است مشروط بر اینکه به‌ازای هر $a,b \in R$ ،

$$f(a + b) = f(a) + f(b) \quad \text{و} \quad f(ab) = f(a)f(b) .$$

تبصره . به‌آسانی دیده‌می‌شود که ردهٔ تمام حلقه‌ها همراه با تمام همریختیهای حلقه‌ها یک رسته (ملموس) تشکیل می‌دهد .

وقتی از قراین معلوم باشد ، اغلب به جای "همریختی حلقه‌ها" می‌نویسیم "همریختی" . یک همریختی حلقه‌ها ، در حالت خاص ، همریختیی از گروههای جمعی زمینه می‌باشد . درنتیجه ، اصطلاحات مشابهی به کار می‌رود :

یک ***تکریختی*** | ***برووریختی*** ، ***یکریختی*** | ***از حلقه‌ها*** یک‌همریختی از حلقه‌ها است که نگاشتی انژکتیو [سورژکتیو ، بیژکتیو] باشد . یک‌تکریختی $R \to S$ از حلقه‌ها را گاهی یک ***نشانندهٔ*** R در S می‌نامند . هر یکریختی $R \to R$ یک ***خودریختی*** R نام دارد .

هستهٔ همریختی $f : R \to S$ از حلقه‌ها هستهٔ آن به عنوان نگاشت گروههای جمعی است ؛ یعنی ، $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$. به همین نحو ، نقش f ، که با $\operatorname{Im} f$ نموده می‌شود ، عبارت است از $\{s \in S \mid s = f(r)\}$ به‌ازای $r \in R$ ی . اگر R و S دارای واحدهای 1_R و 1_S باشند ، لازم ***نیست*** یک همریختی از حلقه‌ها 1_R را به 1_S بنگارد (ر.ک. تمرینات ۱۵ ، ۱۶) .

چند مثال . نگاشت کانونی $\mathbf{Z} \to Z_m$ داده شده با $k \mapsto \bar{k}$ یک برووریختی حلقه‌هاست . نگاشت $Z_3 \to Z_6$ داده شده با $k \mapsto 4k$ یک تکریختی تعریف شده‌ای از حلقه‌هاست .

مثال . فرض کنیم G و H گروههایی ضربی بوده و $f : G \to H$ یک همریختی گروهها باشد . همچنین ، R یک حلقه بوده و نگاشت $\bar{f} : R(G) \to R(H)$ بر حلقه‌های گروهی با

$$\bar{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i)$$

تعریف شده باشد. در این صورت، $\bar{T}$ یک همریختی حلقه‌هاست.

تعریف ۸۰۱. فرض کنیم R یک حلقه باشد. هرگاه کوچکترین عدد صحیح مثبت n که به‌ازای هر $a \in R$، $na = 0$ موجود باشد، آنگاه گوییم R دارای **مشخص** n است. اگر این n موجود نباشد، گوییم R دارای **مشخص صفر** است. (نماد: $char\ R = n$).

قضیهٔ ۹۰۱. *فرض کنیم R حلقه‌ای یکدار با واحد 1_R و مشخص $n > 0$ باشد.*
(یک) هرگاه نگاشت $\varphi : Z \to R$ با $m \mapsto m1_R$ داده شده باشد، آنگاه φ یک همریختی حلقه‌ها با هستهٔ $\langle n \rangle = \{kn \mid k \in Z\}$ است.
(دو) n کوچکترین عدد صحیح مثبتی است که $n1_R = 0$.
(سه) هرگاه R مقسوم‌علیه صفر نداشته باشد (بخصوص، هرگاه R یک دامنهٔ صحیح باشد)، آنگاه n اول است.

طرح برهان. (دو) هرگاه k کوچکترین عدد صحیح مثبتی باشد که $k1_R = 0$، آنگاه، بنابر قضیهٔ ۲۰۱، به‌ازای هر $a \in R$، $ka = k(1_R a) = (k1_R)a = 0 \cdot a = 0$. (سه) هرگاه $n = kr$ که در آن $1 < k < n,\ 1 < r < n$، آنگاه $0 = n1_R = (kr)1_R 1_R = (k1_R)(r1_R)$ ایجاب می‌کند که $k1_R = 0$ یا $r1_R = 0$، که با (دو) متناقض است.

قضیهٔ ۱۰۱. *هر حلقهٔ R را می‌توان در حلقهٔ یکدار S نشانید ـ حلقهٔ S (که منحصر به فرد نیست) را می‌توان با مشخص صفر یا با مشخص حلقهٔ R اختیار کرد.*

طرح برهان. فرض کنیم S گروه آبلی جمعی $R \oplus \mathbf{Z}$ بوده و ضرب در S را با

$$(r_1,k_1)(r_2,k_2) = (r_1r_2 + k_2r_1 + k_1r_2, k_1k_2),\ (r_i \in R;\ k_i \in \mathbf{Z})$$

تعریف می‌کنیم. تحقیق کنید S یک حلقهٔ یکدار با واحد $(0,1)$ و مشخص صفر است و نگاشت $R \to S$ داده شده با $r \mapsto (r,0)$ یک تکریختی حلقه‌ها (نشاننده) است. اگر $\text{char } R = n > 0$، از برهانی مشابه به‌ازای $S = R \oplus Z_n$ و ضرب تعریف شده با

$$(r_1,\bar{k}_1)(r_2,\bar{k}_2) = (r_1r_2 + k_2r_1 + k_1r_2, \bar{k}_1\bar{k}_2)$$

استفاده کنید، که در آن $r_i \in R$ و $\bar{k}_i \in Z_n$ نقش $k_i \in \mathbf{Z}$ تحت‌نگاشت‌کانونی است. در این

صورت، $\operatorname{char} S = n$.

تمرینات

۱. (آ) فرض کنید G یک گروه آبلی (جمعی) باشد. عمل ضرب در G را با $ab = 0$ (به‌ازای هر $a,b, \in G$) تعریف کنید. در این صورت، G یک حلقه است.

(ب) فرض کنید S مجموعهٔ تمام زیرمجموعه‌های مجموعهٔ ثابتی چون U باشد. به‌ازای $A,B \in S$، تعریف کنید $A + B = (A - B) \cup (B - A)$ و $AB = A \cap B$. در این صورت، S یک حلقه است. آیا S تعویضپذیر است؟ آیا S یکدار است؟

۲. فرض کنید $\{R_i \mid i \in I\}$ خانواده‌ای از حلقه‌های یکدار باشد. مجموع مستقیم گروههای آبلی $\sum_{i \in I} R_i$ را با ضرب مختص به مختص به صورت حلقه درآورید. آیا $\sum_{i \in I} R_i$ یکدار است؟

۳. حلقهٔ R که به‌ازای هر $a \in R$، $a^2 = a$ یک **حلقهٔ بولی** نام دارد، ثابت کنید هر حلقهٔ بولی R تعویضپذیر است و به‌ازای هر $a \in R$، $a + a = 0$ [برای نمونه‌ای از یک حلقهٔ بولی، ر.ک. تمرین ۱ (ب) ۱۰]

۴. فرض کنید R یک حلقه و S یک مجموعهٔ ناتهی باشد. در این صورت، گروه $M(S,R)$ (تمرین I ۲.۱۰) حلقه‌ای است که در آن ضرب به صورت زیر تعریف شده است: حاصلضرب $f,g \in M(S,R)$ تابع $S \to R$ است که با $s \mapsto f(s)g(s)$ داده می‌شود.

۵. هرگاه A گروه آبلی $\mathbf{Z} \oplus \mathbf{Z}$ باشد، آنگاه $\operatorname{End} A$ یک حلقهٔ تعویض‌ناپذیر است (ر.ک. ص ۱۸۱).

۶. یک حلقهٔ متناهی (با بیش از یک عنصر) و بدون مقسوم‌علیه صفر یک حلقهٔ بخشی است. (حالت خاص: هر دامنهٔ صحیح متناهی یک میدان است.)

۷. فرض کنید R یک حلقه با بیش از یک عنصر باشد به‌طوری که به‌ازای هر $a \in R$ ناصفر، $b \in R$ ی منحصر به فردی موجود باشد به‌طوری که $aba = a$. ثابت کنید

(آ) R مقسوم‌علیه صفر ندارد؛

(ب) $bab = b$؛

(پ) R یکدار است؛

(ت) R یک حلقهٔ بخشی است.

۸. فرض کنید R مجموعهٔ تمام ماتریسهای 2×2 روی میدان مختلط $\mathbf{C}$ به شکل

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$$

باشد، که در آن $\bar{z},\bar{w}$ به ترتیب مزدوجهای مختلط z و w اند (یعنی، $(c = a + b\sqrt{-1} \Leftrightarrow \bar{c} = a - b\sqrt{-1})$. در این صورت، R یک حلقهٔ بخشی است که با حلقهٔ بخشی K مرکب از چهارتاهای حقیقی یکریخت است. [**راهنمایی.** یکریختی $R \to K$ را با این فرض که نقشهای $1,i,j,k \in K$ به ترتیب ماتریسهای

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

می‌باشند تعریف کنید.

۹. (آ) زیرمجموعهٔ $G = \{1,-1,i,-i,j,-j,k,-k\}$ از حلقهٔ بخشی K از چهارتاهای حقیقی یک گروه تحت ضرب تشکیل می‌دهد.

(ب) G با گروه چهارتایی یکریخت است (تمرینات I ۱۴۰۴۰ و I ۳۰۲۰).

(پ) تفاوت بین حلقهٔ K و حلقهٔ گروهی $\mathbf{R}(G)$ چیست ($\mathbf{R}$ میدان اعداد حقیقی است)؟

۱۰. فرض کنید k,n اعداد صحیحی باشند به‌طوری که $0 \le k \le n$ و $\binom{n}{k}$ ضریب دوجمله‌ای، یعنی $n!/(n-k)!k!$، است، که در آن $0! = 1$ و به‌ازای $n > 0$، $n! = n(n-1)(n-2)\cdots 2\cdot 1$.

(آ) $\binom{n}{k} = \binom{n}{n-k}$

(ب) به‌ازای $k+1 \le n/2$، $\binom{n}{k} < \binom{n}{k+1}$.

(پ) به‌ازای $k < n$، $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

(ت) $\binom{n}{k}$ عددی صحیح است.

(ث) هرگاه p اول بوده و $1 \le k \le p^n - 1$، آنگاه $\binom{p^n}{k}$ بر p بخشپذیر است.

راهنماییها. (ب) توجه کنید که $\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1}$؛ (ت) توجه کنید که $\binom{m}{0} = \binom{m}{m} = 1$ و از استقرا بر n در قسمت (پ) استفاده کنید.]

۱۱ . (رویای دانشجوی تازه‌وارد[1]) . فرض کنید R حلقه‌ای تعویضپذیر و یکدار با مشخص اول p باشد . هرگاه $a,b \in R$ ، آنگاه ، به‌ازای هر عدد صحیح $n \geq 0$ ، $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ [ر.ک. قضیهٔ ۱۰.۶ و تمرین ۱۰ ؛ توجه کنید که اگر $p = 2$ ، $b = -b$] .

۱۲ . عنصر a از یک حلقه **پوچتوان** است اگر به‌ازای n ی ، $a^n = 0$. ثابت کنید در یک حلقهٔ تعویضپذیر $a + b$ پوچتوان است اگر a و b چنین باشند . نشان دهید که این نتیجه در صورت تعویضپذیر نبودن R ممکن است درست نباشد .

۱۳ . در حلقهٔ R ، شرایط زیر معادل یکدیگرند .

(آ) R عنصر پوچتوان ناصفر ندارد (ر.ک. تمرین ۱۲) .

(ب) هرگاه $a \in R$ و $a^2 = 0$ ، آنگاه $a = 0$.

۱۴ . فرض کنید R حلقه‌ای تعویضپذیر و یکدار با مشخص اول p باشد . نگاشت $R \to R$ داده‌شده با $r \mapsto r^p$ یک همریختی حلقه‌هاست که همریختی فروبنیوس[2] نامیده می‌شود [ر.ک. تمرین ۱۱] .

۱۵ . (آ) همریختی ناصفر $f : R \to S$ از حلقه‌های یکدار را طوری مثال بزنید که $f(1_R) \neq 1_S$.

(ب) هرگاه $f : R \to S$ یک‌بروریختی از حلقه‌های یکدار باشد ، آنگاه $f(1_R) = 1_S$.

(پ) هرگاه $f : R \to S$ یک همریختی از حلقه‌های یکدار بوده و u یک یکه در R باشد به‌طوری‌که $f(u)$ یک یکه در S است ، آنگاه $f(1_R) = 1_S$ و $f(u^{-1}) = f(u)^{-1}$.

[**تذکر.** مثالهای ساده‌ای وجود دارند که نشان می‌دهند $f(u)$ ، حتی وقتی u در R یکه است ، لازم نیست یکه باشد .]

۱۶ . فرض کنید $f : R \to S$ یک همریختی حلقه‌ها باشد به‌طوری‌که به‌ازای $r \in R$ ی ناصفر ، $f(r) \neq 0$. هرگاه R یکدار بوده و S مقسوم‌علیه صفر نداشته باشد ، آنگاه S حلقه‌ای یکدار با واحد $f(1_R)$ می‌باشد .

۱۷ . (آ) هرگاه R یک حلقه باشد ، آنگاه R^{op} نیز حلقه است ، که در آن R^{op} چنین تعریف می‌شود . مجموعهٔ زمینهٔ R^{op} همان R بوده و جمع در R^{op} همان جمع در

---

۱ . این اصطلاح از آن وی . او . مک‌برین (V. O. McBrien) است .

2. Frobenius

R است. ضرب در R^{op} ، که با $\circ$ نموده می‌شود ، با $a \circ b = ba$ تعریف می‌گردد ، که در آن ba حاصلضرب در R است. R^{op} **حلقهٔ متقابل** R نام دارد.

(ب) R یکدار است اگر و فقط اگر R^{op} یکدار باشد.

(پ) R یک حلقهٔ بخشی است اگر و فقط اگر R^{op} چنین باشد.

(ت) $(R^{op})^{op} = R$

(ث) هرگاه S حلقه باشد ، آنگاه $R \cong S$ اگر و فقط اگر $R^{op} \cong S^{op}$.

۱۸ . فرض کنید $\mathbf{Q}$ میدان اعداد گویا و R یک حلقه باشد . هرگاه $f,g : \mathbf{Q} \to R$ همریختیهایی از حلقه‌ها باشند به‌طوری که $f|\mathbf{Z} = g|\mathbf{Z}$ ، آنگاه $f = g$. [**راهنمایی** . نشان دهید که به‌ازای $n \in \mathbf{Z}$ $(n \neq 0)$ ، $f(1/n)g(n) = g(1)$ ، که از آنجا $f(1, n) = g(1/n)$.]

۲ ایده‌آلها

همانطور که زیرگروههای نرمال نقشی اساسی در نظریهٔ گروهها دارند ، ایده‌آلها نقش مشابهی در بررسی حلقه‌ها ایفا می‌کنند . ما خواص اساسی ایده‌آلها ، همراه با توصیف ایده‌آلهای اصلی (قضیهٔ ۵۰۲) و قضایای یکریختی مختلفی (۹۰۲ تا ۱۳۰۲ ؛ این قضایا نظیر قضایای یکریختی برای گروهها می‌باشند) ، را عرضه خواهیم کرد ، ایده‌آلهای اول و ماکزیمال به طرق مختلف توصیف می‌شوند . ضربهای مستقیم در رستهٔ حلقه‌ها مطرح شده و قضیهٔ باقیماندهٔ چینی را ثابت خواهیم کرد .

تعریف ۱۰۲ . فرض کنیم R یک حلقه و S زیرمجموعه‌ای ناتهی از R باشد که تحت اعمال جمع و ضرب در R بسته است . هرگاه S خود حلقه‌ای تحت این اعمال باشد ، آنگاه S را یک ***زیرحلقهٔ*** R می‌نامیم . زیرحلقهٔ I از حلقهٔ R یک ***ایده‌آل چپ*** است مشروط بر اینکه

$$x \in I \quad \text{و} \quad r \in R \quad \Rightarrow \quad rx \in I;$$

I ***ایده‌آل راست*** است به شرط آنکه

$$x \in I \quad \text{و} \quad r \in R \quad \Rightarrow \quad xr \in I;$$

I ***ایده‌آل*** است اگر هم ایده‌آل چپ باشد هم ایده‌آل راست .

هروقت حکمی در باب ایده‌آلهای چپ داده شود فرض است که مشابه آن برای

ایده‌آلهای راست برقرار است.

مثال. هرگاه R حلقه باشد، آنگاه **مرکز** R مجموعهٔ

$$C = \{c \in R \mid cr = rc \quad ، \quad r \in R \text{ به‌ازای هر } \}$$

است. به آسانی معلوم می‌شود که C زیرحلقهٔ R است، ولی ممکن است ایده‌آل نباشد (تمرین ۶).

مثال. هرگاه $f : R \to S$ یک همریختی حلقه‌ها باشد، آنگاه $\operatorname{Ker} f$ یک ایده‌آل در R بوده (قضیهٔ ۸.۲ در زیر) و $\operatorname{Im} f$ زیرحلقهٔ S است. $\operatorname{Im} f$ لزوماً ایده‌آلی در S نیست.

مثال. به‌ازای هر عدد صحیح n، زیرگروه دوری $\langle n \rangle = \{kn \mid k \in \mathbf{Z}\}$ یک ایده‌آل در $\mathbf{Z}$ است.

مثال. در حلقهٔ R مرکب از ماتریسهای $n \times n$ روی حلقهٔ بخشی D، I_k را مجموعهٔ تمام ماتریسهایی می‌گیریم که فقط در ستون k درایه‌های ناصفر داشته باشند. در این صورت، I_k یک ایده‌آل چپ است ولی یک ایده‌آل راست نیست. هرگاه J_k از ماتریسهایی تشکیل شده باشد که درایه‌های ناصفرش فقط در سطر k باشند، آنگاه J_k ایده‌آل راست است ولی ایده‌آل چپ نیست.

مثال. دو ایده‌آل از حلقهٔ R عبارتند از خود R و **ایده‌آل بدیهی** (که با 0 نموده می‌شود) که فقط از عنصر صفر تشکیل شده است.

چند تبصره. ایده‌آل [چپ] I از R که $I \neq 0$ و $I \neq R$ یک ***ایده‌آل [چپ] حقیقی*** نامیده می‌شود. توجه کنید که هرگاه R دارای واحد 1_R بوده و I یک ایده‌آل [چپ] R باشد، آنگاه $I = R$ اگر و فقط اگر $1_R \in I$. درنتیجه، ایده‌آل [چپ] ناصفر I از R حقیقی است اگر و فقط اگر I شامل هیچکدام از یکه‌های R نباشد؛ (زیرا هرگاه $u \in R$ یکه بوده و $u \in I$، آنگاه $1_R = u^{-1}u \in I$). بخصوص، حلقهٔ بخشی D ایده‌آل چپ (یا

راست) حقیقی ندارد، زیرا هر عنصر ناصفر D یک یکه می‌باشد. در مورد عکس، ر.ک. تمرین ۷. حلقهٔ ماتریسهای $n \times n$ روی یک حلقهٔ بخشی ایده‌آلهای چپ و راست حقیقی دارد (ر.ک. بالا)، ولی ایده‌آل (دوطرفهٔ) حقیقی ندارد (تمرین ۹).

قضیهٔ ۲.۲. *زیرمجموعهٔ ناتهی I از حلقهٔ R یک ایده‌آل چپ [راست] است اگر و فقط اگر به‌ازای هر $a,b \in I$ و $r \in R$،*

(یک) $a,b \in I \Rightarrow a - b \in I$؛ و

(دو) $a \in I, r \in R \Rightarrow ra \in I$ [$ar \in I$].

برهان. تمرین؛ ر.ک. قضیهٔ ۱.۲.۵.

نتیجهٔ ۳.۲. *فرض کنیم $\{A_i \mid i \in I\}$ خانواده‌ای از ایده‌آلهای [چپ] در حلقهٔ R باشد. در این صورت، $\bigcap_{i \in I} A_i$ نیز یک ایده‌آل [چپ] است.*

برهان. تمرین.

تعریف ۴.۲. فرض کنیم X زیرمجموعه‌ای از حلقهٔ R باشد. همچنین، $\{A_i \mid i \in I\}$ خانوادهٔ تمام ایده‌آلها[ی چپ] در R باشد که شامل X اند. در این صورت، $\bigcap_{i \in I} A_i$ *ایده‌آل [چپ] تولید شده به وسیلهٔ* X نام دارد. این ایده‌آل با (X) نموده می‌شود.

عناصر X *مولدهای* ایده‌آل (X) نام دارند. هرگاه $X = \{x_1, \ldots, x_n\}$، آنگاه ایده‌آل (X) با $(x_1, x_2, \ldots, x_n)$ نموده شده و گوییم *با تولید متناهی* است. ایده‌آل (x) تولید شده به وسیلهٔ یک عنصر یک *ایده‌آل اصلی* نام دارد. یک *حلقهٔ ایده‌آل اصلی* حلقه‌ای است که در آن هر ایده‌آل اصلی است. یک حلقهٔ ایده‌آل اصلی که دامنهٔ صحیح باشد یک دامنهٔ ایده‌آل اصلی نام دارد.[۱]

---

۱. *اصطلاح "حلقهٔ ایده‌آل اصلی" گاهی برای آنچه ما دامنهٔ ایده‌آل اصلی نامیده‌ایم به کار می‌رود.*

قضیهٔ ۵.۲ . فرض کنیم R یک حلقه باشد ، $a \in R$ ، و $X \subset R$.
(یک) ایده‌آل اصلی (a) مرکب است از تمام عناصر به شکل

$$ra + as + na + \sum_{i=1}^{m} r_i a s_i \quad (\; n \in \mathbf{Z} \text{ و } m \in \mathbf{N}^* \text{ ؛ } r,s,r_i,s_i \in R \;) \; .$$

(دو) هرگاه R یکدار باشد ، آنگاه $(a) = \left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R; \, n \in \mathbf{N}^* \right\}$.
(سه) هرگاه a در مرکز R باشد ، آنگاه $(a) = \{ra + na \mid r \in R, n \in \mathbf{Z}\}$.
(چهار) $Ra = \{ra \mid r \in R\}$ [$aR = \{ar \mid r \in R\}$] یک ایده‌آل چپ [راست] در R است (که ممکن است شامل a نباشد) . هرگاه R یکدار باشد ، آنگاه $a \in Ra$ و $a \in aR$.
(پنج) هرگاه R یکدار بوده و a در مرکز R باشد ، آنگاه $Ra = (a) = aR$.
(شش) هرگاه R یکدار بوده و X زیرمجموعهٔ مرکز R باشد ، آنگاه ایده‌آل (X) از تمام مجموعه‌های متناهی $(n \in \mathbf{N}^*; r_i \in R; a_i \in X)$ $r_1 a_1 + \cdots + r_n a_n$ تشکیل شده است .

تبصره. فرض (سه) همواره در یک حلقهٔ تعویضپذیر برقرار است.

طرح برهان ۵.۲ . (یک) نشان دهید که مجموعهٔ

$$I = \left\{ ra + as + na + \sum_{i=1}^{m} r_i a s_i \mid r,s,r_i,s_i \in R; n \in \mathbf{Z}; \, m \in \mathbf{N}^* \right\}$$

ایده‌آلی شامل a است و مشمول هر ایده‌آل شامل a می‌باشد . در این صورت ، $I = (a)$.
قسمت (دو) از اینکه $ra = ra1_R$ ، $as = 1_R as$ ، $na = n(1_R a) = (n1_R)a$ ، و $n1_R \in R$ ، نتیجه می‌شود .

فرض کنیم $A_1, A_2, \ldots, A_n$ زیرمجموعه‌هایی ناتهی از حلقهٔ R باشند . منظور از $A_1 + A_2 + \cdots + A_n$ یعنی مجموعهٔ $\{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i, \, i = 1,2,\ldots,n\}$ به‌ازای اگر A و B زیرمجموعه‌هایی ناتهی از R باشند ، AB را مجموعهٔ تمام مجموعه‌های متناهی $\{a_1 b_1 + \cdots + a_n b_n \mid n \in \mathbf{N}^*; a_i \in A; \, b_i \in B\}$ می‌انگاریم . اگر A فقط از عنصر a تشکیل شده باشد ، به جای AB می‌نویسیم aB . به همین نحو ، اگر $B = \{b\}$ ، به جای AB می‌نویسیم Ab . توجه کنید که هرگاه $A \mid B$ تحت جمع بسته باشد ، آنگاه

$aB = \{ab \mid b \in B\}$ و $Ab = \{ab \mid a \in A\}$]. به‌طور کلی، فرض کنیم $A_1A_2\cdots A_n$ مجموعهٔ تمام مجموعه‌ها از عناصر به شکل $a_1a_2\cdots a_n$ (به‌ازای $a_i \in A_i$ ، $i = 1,2,\ldots,n$) باشد. درحالت خاص، وقتی تمام A_i ها ($1 \le i \le n$) مساوی مجموعهٔ A باشند، $A_1A_2\cdots A_n = A.A\cdots A$ را با A^n نشان می‌دهیم.

قضیهٔ ۶۰۲. *فرض کنیم* $A, A_1, A_2, \ldots, A_n$ ، B ، و C *ایده‌آلهای* [چپ] *در حلقهٔ* R *باشند.*

(یک) $A_1 + A_2 + \cdots + A_n$ و $A_1A_2\cdots A_n$ *ایده‌آلهایی* [چپ] *می‌باشند؛*

(دو) $(A + B) + C = A + (B + C)$ ؛

(سه) $(AB)C = ABC = A(BC)$ ؛

(چهار) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots BA_n$ ؛ و

$(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

طرح برهان. برای (یک) از قضیهٔ ۲۰۲ استفاده کنید. قسمت (سه) کمی مشکل است ولی استدلال سرراستی با استفاده از تعاریف دارد. با استفاده از استقرا، قسمت (چهار) را، ابتدا با نشان دادن اینکه $A(B + C) = AB + AC$ و $(A + B)C = AC + BC$، ثابت کنید.

ایده‌آلها تقریبا " همان نقش در نظریهٔ حلقه‌ها را دارند که زیرگروههای نرمال در نظریهٔ گروهها ایفا می‌کنند. مثلا "، فرض کنیم R حلقه و I ایده‌آلی از R باشد. چون گروه جمعی R آبلی‌است، I زیرگروه‌نرمالی‌می‌باشد. درنتیجه، طبق قضیهٔ ۴۰۵۰ I ، گروه خارج قسمتی R/I وجود دارد، که در آن جمع به صورت زیر تعریف شده است:

$$(a + I) + (b + I) = (a + b) + I.$$

درواقع، R/I را می‌توان به یک حلقه تبدیل کرد.

قضیهٔ ۷۰۲. *فرض کنیم* R *یک حلقه و* I *ایده‌آلی از* R *باشد. در این صورت، گروه خارج قسمتی جمعی* R/I *حلقه‌ای است که در آن ضرب به صورت زیر داده می‌شود:*

$$(a + I)(b + I) = ab + I.$$

هرگاه R تعویضپذیر بوده یا یکدار باشد، همین امر برای R/I نیز درست است.

طرح برهان ۷۰۲. اگر نشان دهیم ضرب در R/I تعریف شده است، اثبات حلقه بودن R/I امری عادی می‌شود. (مثلاً، هرگاه R دارای واحد 1_R باشد، آنگاه $1_R + I$ واحد در R/I می‌باشد.) فرض کنیم $a + I = a' + I$ و $b + I = b' + I$. باید نشان دهیم که $ab + I = a'b' + I$. چون $a' \in a' + I = a + I$، به‌ازای $i \in I$ ی، $a' = a + i$. به همین نحو، به‌ازای $j \in I$ ی، $b' = b + j$. درنتیجه،

$$a'b' = (a + i)(b + j) = ab + ib + aj + ij.$$

چون I ایده‌آل است،

$$a'b' - ab = ib + aj + ij \in I.$$

لذا، طبق نتیجهٔ ۳۰۴۰۱، $a'b' + I = ab + I$؛ یعنی، ضرب در R/I تعریف شده است.

ممکن است به خاطر تشابه با گروهها انتظار داشت که ایده‌آلها و همریختیهای حلقه‌ها رابطهٔ نزدیکی باهم داشته باشند.

قضیهٔ ۸۰۲. هرگاه $f : R \to S$ یک همریختی حلقه‌ها باشد، آنگاه هستهٔ f ایده‌آلی در R است. به عکس، هرگاه I ایده‌آلی در R باشد، آنگاه نگاشت $\pi : R \to R/I$ داده شده با $r \mapsto r + I$ یک بروریختی حلقه‌ها با هستهٔ I است.

نگاشت π ***بروریختی کانونی*** (یا تصویر) نام دارد.

برهان ۸۰۲. $\operatorname{Ker} f$ یک زیرگروه جمعی R است. هرگاه $x \in \operatorname{Ker} f$ و $r \in R$، آنگاه $f(rx) = f(r)f(x) = f(r)0 = 0$، که از آنجا $rx \in \operatorname{Ker} f$. به همین نحو، $xr \in \operatorname{Ker} f$. بنابراین، $\operatorname{Ker} f$ یک ایده‌آل است. بنابر قضیهٔ ۵۰۵۰۱، نگاشت π یک بروریختی گروهها با هستهٔ I است. چون به‌ازای هر $a, b \in R$، $\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$، π نیز یک بروریختی حلقه‌ها می‌باشد.

در پرتو نتایج پیش، برقراری قضایای مختلف یکریختی گروهها (قضایای ۶.۵.۱ تا ۱۲.۵.۱)، که در آنها به‌جای *زیرگروههای نرمال وگروهها* به ترتیب *ایده‌آلها و حلقه‌ها* گذارده‌ایم، در مورد حلقه‌ها تعجبی نخواهد داشت. در هر حالت، وجود یکریختی مطلوب برای گروههای آبلی جمعی دانسته فرض می‌شود. هرگاه گروههای مربوطه حلقه و زیرگروههای نرمال ایده‌آل باشند، آنگاه لازم است فقط تحقیق شود که یکریختی معلوم در مورد گروهها یک همریختی، و درنتیجه یک یکریختی حلقه‌ها، نیز هست. **اخطار.** در برهان قضایای یکریختی برای گروهها، تمام گروهها و هم‌مجموعه‌ها به صورت ضربی نوشته می‌شوند، ولی گروه‌جمعی یک حلقه و هم‌مجموعه‌های یک ایده‌آل به‌طور جمعی نوشته خواهند شد.

قضیهٔ ۹.۲. *هرگاه $f:R\to S$ یک همریختی حلقه‌ها بوده و I ایده‌آلی از R باشد که مشمول هستهٔ f است، آنگاه همریختی منحصر به فردی از حلقه‌ها مانند $\bar{f}:R/I\to S$ وجود دارد به‌طوری که به‌ازای هر $a\in R$، $\bar{f}(a+I)=f(a)$. و $Im\,\bar{f}=Im\,f$. $\bar{f}$ یک یکریختی است اگر و فقط اگر f یک برووریختی بوده و $Ker\,\bar{f}=(Ker\,f)/I$. $I=Ker\,f$.*

برهان. تمرین؛ ر.ک. قضیهٔ ۶.۵.۱.

نتیجهٔ ۱۰.۲ (قضیهٔ اول یکریختی). *هرگاه $f:R\to S$ یک همریختی حلقه‌ها باشد، آنگاه f یک یکریختی حلقه‌ها مانند $R/Ker\,f\cong Im\,f$ را القا خواهد کرد.*

برهان. تمرین؛ ر.ک. نتیجهٔ ۷.۵.۱.

نتیجهٔ ۱۱.۲. *هرگاه $f:R\to S$ یک همریختی حلقه‌ها، I ایده‌آلی در R، و J ایده‌آلی در S باشد به‌طوری که $f(I)\subset J$، آنگاه f یک همریختی حلقه‌ها مانند $\bar{f}:R/I\to S/J$ را القا می‌کند که با $a+I\mapsto f(a)+J$ داده می‌شود. $\bar{f}$ یکریختی است اگر و فقط اگر $Im\,f+J=S$ و $f^{-1}(J)\subset I$. بخصوص، هرگاه f یک برووریختی باشد به‌طوری که $f(I)=J$ و $Ker\,f\subset I$، آنگاه $\bar{f}$ یکریختی می‌باشد.*

برهان. تمرین؛ ر.ک. نتیجهٔ I ۸۰۵۰ .

قضیهٔ ۱۲۰۲ . *فرض کنیم* I و J *ایده‌آلهایی در حلقهٔ* R *باشند* .
(یک) (قضیهٔ دوم یکریختی) *یک یکریختی حلقه‌ها مانند* $I/(I \cap J) \cong (I+J)/J$ *وجود دارد*؛
(دو) (قضیهٔ سوم یکریختی) *هرگاه* $I \subset J$ ، *آنگاه* J/I *ایده‌آلی در* R/I *است و یک یکریختی حلقه‌ها مانند* $R/J \cong (R/I)/(J/I)$ *وجود دارد* .

برهان. تمرین؛ ر.ک. نتایج I ۹۰۵۰ و I ۱۰۰۵۰ .

قضیهٔ ۱۳۰۲ . *هرگاه* I *ایده‌آلی در حلقهٔ* R *باشد ، آنگاه تناظری یک به یک بین مجموعهٔ تمام ایده‌آلهای* R *که شامل* I *اند و مجموعهٔ تمام ایده‌آلهای* R/I *موجود می‌باشد که با* $J \mapsto J/I$ *داده شده است . از اینرو ، هر ایده‌آل در* R/I *به شکل* J/I *است ، که در آن* J *ایده‌آلی از* R *است که شامل* I *می‌باشد* .

برهان. تمرین؛ ر.ک. قضیهٔ I ۱۱۰۵۰ ، نتیجهٔ I ۱۲۰۵۰ ، و تمرین ۱۳ .

حال دو نوع ایده‌آل (اول و ماکزیمال) را که اغلب مورد توجه‌اند به چند طریق توصیف می‌کنیم .

تعریف ۱۴۰۲ . ایده‌آل P در حلقهٔ R را **اول** گوییم اگر $P \neq R$ و به‌ازای هر ایده‌آل A,B در R

$$AB \subset P \Rightarrow B \subset P \text{ یا } A \subset P.$$

تعریف ایده‌آل اول ، ایده‌آل R را هم به دلیل تاریخی و هم تکنیکی مستثنی کرده است . در اینجا توصیف بسیار مفیدی از ایده‌آلهای اول داده شده است؛ توصیفهای دیگر در تمرین ۱۴ خواهند آمد .

قضیهٔ ۱۵۰۲ . *هرگاه* P *ایده‌آلی در حلقهٔ* R *باشد به‌طوری که* $P \neq R$ *و به‌ازای هر*

، $a,b\in R$

(۱) $$ab\in P \Rightarrow b\in P \text{ یا } a\in P,$$

آنگاه P اول است. به عکس، هرگاه P اول و R تعویضپذیر باشد، آنگاه P در شرط (۱) صدق می‌کند.

تبصره. برای عکس قضیه، تعویضپذیری لازم است (تمرین ۹ (ب)).

برهان ۱۵۰۲. هرگاه A و B ایده‌آلهایی باشند به‌طوری که $AB\subset P$ و $A\not\subset P$، آنگاه عنصری مانند $a\in A-P$ وجود دارد. به‌ازای هر $b\in B$، $ab\in AB\subset P$، که از آنجا $a\in P$ یا $b\in P$. چون $a\notin P$، باید به‌ازای هر $b\in B$، $b\in P$؛ یعنی، $B\subset P$. بنابراین، P اول است. به عکس، هرگاه P یک ایده‌آل بوده و $ab\in P$، آنگاه، طبق تعریف ۴۰۲، ایده‌آل اصلی (ab) مشمول P است. هرگاه R تعویضپذیر باشد، آنگاه قضیهٔ ۵۰۲ ایجاب می‌کند که $(a)(b)\subset(ab)$، که از آنجا $(a)(b)\subset P$. هرگاه P اول باشد، آنگاه $(a)\subset P$ یا $(b)\subset P$، که از آنجا $a\in P$ یا $b\in P$.

چند مثال. ایده‌آل صفر در یک دامنهٔ صحیح اول است، زیرا $ab=0$ اگر و فقط اگر $a=0$ یا $b=0$. هرگاه p عدد صحیح اولی باشد، آنگاه ایده‌آل اصلی (p) در $\mathbf{Z}$ اول است، زیرا

$$ab\in(p) \Rightarrow p\mid ab \Rightarrow p\mid b \text{ یا } p\mid a \Rightarrow b\in(p) \text{ یا } a\in(p).$$

قضیهٔ ۱۶۰۲. *در حلقهٔ تعویضپذیر R دارای واحد $1_R\neq 0$ ایده‌آل P اول است اگر و فقط اگر حلقهٔ خارج قسمتی R/P دامنهٔ صحیح باشد.*

برهان. بنابر قضیهٔ ۷۰۲، R/P یک حلقهٔ تعویضپذیر دارای واحد 1_R+P و عنصر صفر $0+P=P$ است. هرگاه P اول باشد، آنگاه $1_R+P\neq P$، زیرا $P\neq R$. به علاوه، R/P مقسوم‌علیه صفر ندارد، زیرا

$$(a+P)(b+P)=P \Rightarrow ab+P=P \Rightarrow ab\in P \Rightarrow a\in P \text{ یا } b\in P \Rightarrow a+P=P \text{ یا } b+P=P$$

بنابراین، R/P دامنهٔ صحیح است. به عکس، هرگاه R/P دامنهٔ صحیح باشد، آنگاه $1_R + P \neq 0 + P$، که از آنجا $1_R \notin P$. بنابراین، $P \neq R$. چون R/P مقسوم‌علیه صفر ندارد،

$$ab \in P \rightarrow ab + P = P \rightarrow (a + P)(b + P) = P \rightarrow a + P = P$$

$$b + P = P \rightarrow a \in P \text{ یا } b \in P$$

بنابراین، طبق قضیهٔ ۱۵۰۲، P اول است.

تعریف ۱۷۰۲. ایده‌آل [چپ] M درحلقهٔ R را *ماکزیمال* گوییم اگر $M \neq R$ و به‌ازای هر ایده‌آل [چپ] N که $M \subset N \subset R$، یا $N = M$ یا $N = R$.

مثال. ایده‌آل (3) در $\mathbf{Z}$ ماکزیمال است، ولی ایده‌آل (4) نیست، زیرا $(4) \subsetneq (2) \subsetneq \mathbf{Z}$.

تبصره. هرگاه R حلقه و $\mathcal{S}$ مجموعهٔ تمام ایده‌آلهای [از] R باشد که $I \neq R$، آنگاه $\mathcal{S}$ به وسیلهٔ شمول نظریهٔ مجموعه‌ها جزئی مرتب است. M یک ایده‌آل ماکزیمال است (تعریف ۱۷۰۲) اگر و فقط اگر M در مجموعهٔ جزئی مرتب $\mathcal{S}$ به معنی آمده درآشنایی، بخش ۷، یک عنصر ماکزیمال باشد. به‌طور کلی، گاهی ایده‌آل I را نسبت به خاصیتی ماکزیمال گویند بدین معنی که، تحت ترتیب جزئی شمول نظریهٔ مجموعه‌ها، I در مجموعهٔ تمام ایده‌آلهای R واجد خاصیت داده شده ماکزیمال است. در این حالت، I لازم نیست به معنی تعریف ۱۷۰۲ ماکزیمال باشد.

قضیهٔ ۱۸۰۲. در حلقهٔ ناصفر و یکدار R همواره ایده‌آلهای [چپ] ماکزیمال وجود دارند. درواقع، هر ایده‌آل [چپ] در R (جز خود R) مشمول یک ایده‌آل [چپ] ماکزیمال است.

برهان. چون 0 یک ایده‌آل است و $R \neq 0$، کافی است حکم دوم را ثابت کنیم. برهان کاربرد سرراست لم زرن است. اگر A یک ایده‌آل [چپ] در R باشد به‌طوری که $A \neq R$، $\mathcal{S}$ را مجموعهٔ تمام ایده‌آلهای [چپ] B در R می‌گیریم که $A \subset B \neq R$. $\mathcal{S}$ ناتهی است، زیرا $A \in \mathcal{S}$. $\mathcal{S}$ را با شمول نظریهٔ مجموعه‌ها جزئی مرتب می‌کنیم (یعنی، $B_1 \leq B_2 \Leftrightarrow B_1 \subset B_2$). برای اعمال لم زرن باید نشان داد که هر زنجیر $\mathcal{C} = \{C_i \mid i \in I\}$

از ایده‌آلها [چپ] در S کران بالایی در S دارد. فرض کنیم $C = \bigcup_{i\in I} C_i$. حکم می‌کنیم C یک ایده‌آل [چپ] است. هرگاه $a,b\in C$، آنگاه به‌ازای $i,j\in I$ ی، $a\in C_i$ و $b\in C_j$. چون $\mathcal{C}$ یک زنجیر است، $C_i\subset C_j$ یا $C_j\subset C_i$. فرض کنیم آخری برقرار باشد. از اینرو، $a,b\in C_j$. چون C_j یک ایده‌آل چپ است، $a-b\in C_j$ و، به‌ازای هر $r\in R$، $ra\in C_j$ (اگر C_j یک ایده‌آل باشد، نیز $ar\in C_j$). بنابراین، $a,b\in C$ ایجاب می‌کند که $a-b$ و ra در $C_j\subset C$ باشند. درنتیجه، طبق قضیهٔ ۲۰۲، C یک ایده‌آل [چپ] است. چون به‌ازای هر i، $A\subset C_i$، و چون هر C_i در S است، $A\subset \bigcup C_i = C$. درنتیجه، به‌ازای هر $i\in I$، $C_i\neq R$ (در غیر این صورت، $1_R\notin C_i$). درنتیجه، به‌ازای هر i، $C_i = R$)، که از آنجا $1_R\notin \bigcup C_i = C$. بنابراین، $C\neq R$؛ و درنتیجه، $C\in S$. واضح است که C یک کران بالایی زنجیر $\mathcal{C}$ است. لذا، مفروضات لم‌زرن برقرارند؛ و درنتیجه، S شامل عنصر ماکزیمال است. اما یک عنصر ماکزیمال S بوضوح یک ایده‌آل [چپ] ماکزیمال در R و شامل A است.

قضیهٔ ۱۹۰۲. ***هرگاه R یک حلقهٔ تعویضپذیر باشد به‌طوری که $R^2 = R$ (بخصوص، هرگاه R یکدار باشد)، آنگاه هر ایده‌آل ماکزیمال M در R اول است.***

تبصره. عکس قضیهٔ ۱۹۰۲ درست نیست. مثلاً "، 0 یک ایده‌آل اول در $\mathbf{Z}$ است، ولی یک ایده‌آل ماکزیمال نیست. همچنین، ر.ک. تمرین ۹.

برهان ۱۹۰۲. فرض کنیم $ab\in M$ ولی $a\notin M$ و $b\notin M$. در این صورت، هر یک از ایده‌آلهای $M+(a)$ و $M+(b)$ حقیقتاً " شامل M است. بنابر ماکزیمالی، $M+(a) = R = M+(b)$. چون R تعویضپذیر بوده و $ab\in M$، قضیهٔ ۵۰۲ ایجاب می‌کند که $(a)(b)\subset (ab)\subset M$. بنابراین،

$$R = R^2 = (M+(a))(M+(b))\subset M^2 + (a)M + M(b) + (a)(b)\subset M.$$

این با این امر که $M\neq R$ تعارض دارد (زیرا M ماکزیمال است). بنابراین، $a\in M$ یا $b\in M$، که از آنجا، طبق قضیهٔ ۱۵۰۲، M اول است.

ایده‌آلهای ماکزیمال را، مانند ایده‌آلهای اول، می‌توان برحسب حلقه‌های خارج

قسمتی آنها توصیف کرد .

قضیهٔ ۲۰۰۲ . *فرض کنیم* M *ایده‌آلی در حلقهٔ یکدار* R *با واحد* $1_R \neq 0$ *باشد .*
(یک) *هرگاه* M *ماکزیمال و* R *تعویضپذیر باشد ، آنگاه حلقهٔ خارج قسمتی* R/M *یک میدان است .*
(دو) *هرگاه حلقهٔ خارج قسمتی* R/M *یک حلقهٔ بخشی باشد ، آنگاه* M *ماکزیمال است .*

چند تبصره . در صورتی که R یکدار نباشد (یک) درست نیست . (تمرین ۱۹) . هرگاه M ماکزیمال بوده و R تعویضپذیر نباشد ، آنگاه R/M لزوما" یک حلقهٔ بخشی نیست (تمرین ۹) .

برهان ۲۰۰۲ . (یک) هرگاه M ماکزیمال باشد ، آنگاه M اول است (قضیهٔ ۱۹۰۲) ، که از آنجا ، طبق قضیهٔ ۱۶۰۲ ، R/M یک دامنهٔ صحیح است . لذا ، کافی است نشان دهیم هرگاه $a + M \neq M$ ، آنگاه $a + M$ یک معکوس ضربی در R/M دارد . اما $a + M \neq M$ ایجاب می‌کند که $a \notin M$ ، که از آنجا M حقیقتا" مشمول ایده‌آل $M + (a)$ است . چون M ماکزیمال است ، باید داشته باشیم $M + (a) = R$. بنابراین ، چون R تعویضپذیر است ، طبق قضیهٔ ۵۰۲ (پنج) ، به‌ازای $m \in M$ و $r \in R$ ی ، $1_R = m + ra$. لذا ، $1_R - ra = m \in M$ ، که از آنجا

$$1_R + M = ra + M = (r + M)(a + M).$$

لذا ، $r + M$ یک معکوس ضربی $a + M$ در R/M است ، درنتیجه R/M میدان می‌باشد .
(دو) هرگاه R/M یک حلقهٔ بخشی باشد ، آنگاه $1_R + M \neq 0 + M$ ، که از آنجا $1_R \notin M$ و $M \neq R$. اگر N یک ایده‌آل باشد به‌طوری که $M \subsetneq N$ ، فرض می‌کنیم $a \in N - M$. در این صورت ، $a + M$ دارای معکوس ضربی در R/M است ؛ مثلا" ، $(a + M)(b + M) = 1_R + M$. درنتیجه ، $ab + M = 1_R + M$ و $ab - 1_R = c \in M$. اما $a \in N$ و $M \subset N$ ایجاب می‌کنند که $1_R \in N$. لذا ، $N = R$. بنابراین ، M ماکزیمال است .

نتیجهٔ ۲۱۰۲ . *شرایط زیر بر حلقهٔ تعویضپذیر و یکدار* R *با واحد* $1_R \neq 0$ *معادلند :*

(یک) R میدان است؛
(دو) R ایده‌آل حقیقی ندارد؛
(سه) 0 ایده‌آل ماکزیمال در R است؛
(چهار) هر همریختی ناصفر $R \to S$ از حلقه‌ها یک تکریختی است.

تبصره. مشابه نتیجهٔ ۲۱۰۲ برای حلقه‌های بخشی درست نیست (تمرین ۹).

برهان ۲۱۰۲. این نتیجه را می‌توان مستقیماً (تمرین ۷) یا به صورت زیر ثابت کرد. بنابر قضیهٔ ۲۰۰۲، $R \cong R/0$ میدان است اگر و فقط اگر 0 ماکزیمال باشد. اما 0 بوضوح ماکزیمال است اگر و فقط اگر R ایده‌آل حقیقی نداشته باشد. بالاخره، به‌ازای هر ایده‌آل I $(\neq R)$، نگاشت کانونی $\pi : R \to R/I$ یک همریختی ناصفر با هستهٔ I است (قضیهٔ ۸۰۲). چون π تکریختی است اگر و فقط اگر $I = 0$، (چهار) برقرار است اگر و فقط اگر R ایده‌آل حقیقی نداشته باشد.

حال حاصلضربها (ی مستقیم) در رستهٔ حلقه‌ها را درنظر می‌گیریم. وجود و خواص اساسی آنها به آسانی، با استفاده از خواص نظیر برای گروهها، ثابت می‌شوند. اما هم حاصلضربهای حلقه‌ها مشکلتر است. به علاوه، هم حاصلضربها در رستهٔ حلقه‌ها، مثلاً، از هم حاصلضربها (مجموعه‌های مستقیم) در رستهٔ گروههای آبلی کمتر مورد استعمال دارند.

قضیهٔ ۲۲۰۲. فرض کنیم $\{R_i \mid i \in I\}$ یک خانوادهٔ ناتهی از حلقه‌ها بوده و $\prod_{i \in I} R_i$ حاصلضرب مستقیم گروههای آبلی جمعی R_i ها باشد.

(یک) $\prod_{i \in I} R_i$ یک حلقه است با ضربی که به صورت $\{a_i\}_{i \in I} \{b_i\}_{i \in I} = \{a_i b_i\}_{i \in I}$ تعریف شده است.

(دو) هرگاه R_i، به‌ازای هر $i \in I$، یکدار [تعویضپذیر] باشد، آنگاه $\prod_{i \in I} R_i$ نیز یکدار [تعویضپذیر] است.

(سه) به‌ازای هر $k \in I$، تصویر کانونی $\pi_k : \prod_{i \in I} R_i \to R_k$ داده شده با $\{a_i\} \mapsto a_k$ یک برووریختی از حلقه‌ها می‌باشد.

(چهار) به‌ازای هر $k \in I$ ، انژکسیون کانونی $\iota_k : R_k \to \coprod_{i\in I} R_i$ داده‌شده با $a_k \mapsto \{a_i\}$ (که به‌ازای $i \neq k$ ، $a_i = 0$) یک تکریختی حلقه‌هاست.

برهان. تمرین.

$\coprod_{i\in I} R_i$ حاصل‌ضرب مستقیم (خارجی) خانواده‌ٔ $\{R_i \mid i \in I\}$ از حلقه‌ها نامیده می‌شود. هرگاه مجموعه‌ٔ اندیسگذار متناهی باشد، مثلا" $I = \{1, \ldots, n\}$ ، آنگاه گاهی به جای $\coprod R_i$ می‌نویسیم $R_1 \times R_2 \times \cdots \times R_n$.

هرگاه $\{R_i \mid i \in I\}$ خانواده‌ای از حلقه‌ها بوده و به‌ازای هر $i \in I$ ، A_i ایده‌آلی در R_i باشد، آنگاه به‌آسانی معلوم می‌شود که $\coprod_{i\in I} A_i$ یک ایده‌آل در $\coprod_{i\in I} R_i$ است. هرگاه به‌ازای هر $i \neq k$ ، $A_i = 0$ ، آنگاه ایده‌آل $\coprod_{i\in I} A_i$ دقیقا" $\iota_k(A_k)$ است. هرگاه مجموعه‌ٔ اندیسگذار I متناهی بوده و هر R_i واحد داشته باشد، آنگاه هر ایده‌آل در $\coprod_{i\in I} R_i$ به شکل $\coprod_{i\in I} A_i$ است، که در آن هر A_i یک ایده‌آل در R_i است (تمرین ۲۲).

قضیه‌ٔ ۲۳۰۲ . *فرض کنیم $\{R_i \mid i \in I\}$ یک‌خانواده‌ٔ ناتهی از حلقه‌ها، S یک حلقه، و $\{\varphi_i : S \to R_i \mid i \in I\}$ خانواده‌ای از همریختیهای حلقه‌ها باشد. در این صورت، یک همریختی منحصر به فرد از حلقه‌ها مانند $\varphi : S \to \coprod_{i\in I} R_i$ وجود دارد به‌طوری که به‌ازای هر $i \in I$ ، $\pi_i\varphi = \varphi_i$. این خاصیت حلقه‌ٔ $\coprod_{i\in I} R_i$ را به‌طور منحصر به فرد با تقریب یکریختی معین می‌کند. به عبارت دیگر، $\coprod_{i\in I} R_i$ یک حاصل‌ضرب در رسته‌ٔ حلقه‌ها می‌باشد.*

طرح برهان. بنابر قضیه‌ٔ ۲۰۸۰ I ، همریختی منحصر به فردی از گروهها مانند $\varphi : S \to \coprod_{i\in I} R_i$ وجود دارد به‌طوری‌که به‌ازای هر $i \in I$ ، $\pi_i\varphi = \varphi_i$. تحقیق کنید که φ نیز یک همریختی حلقه‌هاست. لذا، $\coprod_{i\in I} R_i$ یک حاصل‌ضرب در رسته‌ٔ حلقه‌هاست (تعریف ۲۰۷۰ I)؛ و لذا، طبق قضیه‌ٔ ۳۰۷۰ I ، با تقریب یکریختی معین می‌شود.

قضیه‌ٔ ۲۴۰۲ . *فرض کنیم $A_1, A_2, \ldots, A_n$ ایده‌آلهایی در حلقه‌ٔ R باشند به‌طوری که (یک) $A_1 + A_2 + \cdots + A_n = R$ و (دو) به‌ازای هرمقدار k $(1 \leq k \leq n)$ ،*

$A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots + A_n) = 0$. ***در این صورت ، یک یکریختی حلقه‌ها مانند*** $R \cong A_1 \times A_2 \times \cdots \times A_n$ ***وجود دارد .***

برهان . طبق برهان قضیهٔ I ۶.۸.۰ ، نگاشت $\varphi : A_1 \times A_2 \times \cdots \times A_n \to R$ داده شده با $(a_1, \ldots, a_n) \mapsto a_1 + a_2 + \cdots + a_n$ یک یکریختی از گروههای آبلی جمعی است . کافی است تحقیق کنیم که φ یک همریختی حلقه‌هاست . ملاحظه کنید که هرگاه $i \neq j$ و $a_i \in A_i, a_j \in A_j$ ، آنگاه ، بنابر قسمت (دو) ، $a_i a_j \in A_i \cap A_j = 0$. درنتیجه ، به‌ازای هر $a_i, b_i \in A_i$ ،

$$(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = a_1 b_1 + \cdots + a_n b_n,$$

که از آنجا φ یک همریختی حلقه‌ها می‌باشد .

هرگاه R حلقه بوده و $A_1, \ldots, A_n$ ایده‌آلهایی در R باشند که در مفروضات قضیهٔ ۲۴۰۲ صدق می‌کنند ، آنگاه گوییم R ***حاصلضرب مستقیم (داخلی)*** ایده‌آلهای A_i است . مثل حالت گروهها ، تمایزی بین حاصلضربهای مستقیم داخلی و خارجی وجود دارد . هر گاه حلقهٔ R حاصلضرب مستقیم ***داخلی*** ایده‌آلهای $A_1, \ldots, A_n$ باشد ، آنگاه هر A_i عملا" یک ایده‌آل مشمول R بوده و R با حاصلضرب مستقیم ***خارجی یکریخت*** است . اما حاصلضرب مستقیم خارجی $A_1 \times \cdots \times A_n$ شامل A_i ***نیست*** ، بلکه فقط نسخه‌های یکریختی از آنها را شامل است (یعنی ، $\iota_i(A_i)$ ها را ــ ر.ک. قضیهٔ ۲۲۰۲) . چون این تمایز عملا" مهم نیست ، وقتی از قراین معلوم باشد ، صفات "داخلی" و "خارجی" را حذف کرده و از نمادگذاری زیر استفاده خواهیم کرد .

نمادگذاری . برای آنکه نشان دهیم حلقهٔ R حاصلضرب مستقیم داخلی ایده‌آلهای $A_1, \ldots, A_n$ خود است ، می‌نویسیم $R = \prod A_i$ یا $R = A_1 \times A_2 \times \cdots \times A_n$.

توصیفهای دیگر حاصلضربهای مستقیم متناهی در تمرین ۲۴ داده شده‌اند .

این بخش را با نتیجه‌ای که در فصلهای هشت و نه لازم می‌شود به پایان می‌بریم . فرض کنیم A یک ایده‌آل در حلقهٔ R بوده و $a, b \in R$. گوییم عنصر a با b ***همنهشت*** به پیمانهٔ A است (که با $a \equiv b \pmod{A}$ نموده می‌شود) اگر $a - b \in A$. لذا ،

$$a \equiv b \pmod{A} \iff a - b \in A \iff a + A = b + A.$$

چون R/A طبق قضیهٔ ۷۰۲ حلقه است،

$$b_1 \equiv b_2 \pmod{A} \quad \text{و} \quad a_1 \equiv a_2 \pmod{A} \quad \Rightarrow$$
$$a_1 b_1 \equiv a_2 b_2 \pmod{A} \quad \text{و} \quad a_1 + b_1 \equiv a_2 + b_2 \pmod{A}$$

قضیهٔ ۲۵۰۲ (قضیهٔ باقیماندهٔ چینی). فرض کنیم $A_1, \ldots, A_n$ ایده‌آلهایی در حلقهٔ R باشند به‌طوری‌که به‌ازای هر i، $R^2 + A_i = R$ و به‌ازای هر $j \neq i$، $A_i + A_j = R$. هرگاه $b_1, \ldots, b_n \in R$، آنگاه $b \in R$ ای وجود دارد به‌طوری‌که

$$b \equiv b_i \ (mod\ A_i) \qquad (i = 1, 2, \ldots, n).$$

به علاوه، b با تقریب همنهشتی به پیمانهٔ ایده‌آل

$$A_1 \cap A_2 \cap \cdots \cap A_n$$

به‌طور منحصر به فرد معین می‌شود.

تبصره. هرگاه R یکدار باشد، آنگاه $R^2 = R$، که ازآنجا، به‌ازای هر ایده‌آل A از R، $R^2 + A = R$.

طرح برهان ۲۵۰۲. چون $A_1 + A_2 = R$ و $A_1 + A_3 = R$،

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3$$
$$\subset A_1 + A_2A_3 \subset A_1 + (A_2 \cap A_3).$$

درنتیجه، چون $R = A_1 + R^2$،

$$R = A_1 + R^2 \subset A_1 + (A_1 + (A_2 \cap A_3)) = A_1 + (A_2 \cap A_3) \subset R.$$

بنابراین، $R = A_1 + (A_2 \cap A_3)$. به استقرا فرض کنیم

$$R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1}).$$

در این صورت،

$$R^2 = (A_1 + (A_2 \cap \cdots \cap A_{k-1}))(A_1 + A_k) \subset A_1 + (A_2 \cap A_3 \cap \cdots \cap A_k)$$

و درنتیجه،

$$R = R^2 + A_1 \subset A_1 + (A_2 \cap \cdots \cap A_k) \subset R.$$

لذا، $R = A_1 + (A_2 \cap \cdots \cap A_k)$ و مرحلهٔ استقرا ثابت شده است. درنتیجه،

$R = A_1 + (A_2 \cap \cdots \cap A_n) = A_1 + (\bigcap_{i\neq 1} A_i)$. استدلالی مشابه نشان می‌دهد که به‌ازای هر $k = 1,2,\ldots,n$ ، عناصری مانند $R = A_k + (\bigcap_{i\neq k} A_i)$. درنتیجه ، به‌ازای هر k ، $a_k \in A_k$ و $r_k \in \bigcap_{i\neq k} A_i$ وجود دارند به‌طوری که $b_k = a_k + r_k$. به علاوه ، به‌ازای $i \neq k$ ، $r_k \equiv b_k \pmod{A_k}$ و $r_k \equiv 0 \pmod{A_i}$.

فرض کنید $b = r_1 + r_2 + \cdots + r_n$ و ، با استفاده از تبصره‌های پیش از قضیه ، ثابت کنید به‌ازای هر i ، $b \equiv b_i \pmod{A_i}$. بالاخره ، هرگاه $c \in R$ چنان باشد که به‌ازای هر i ، $c \equiv b_i \pmod{A_i}$ ، آنگاه به‌ازای هر i ، $b \equiv c \pmod{A_i}$ ، که از آنجا به‌ازای هر i ، $b - c \in A_i$. بنابراین ، $b \equiv c \left(\mathrm{mod} \bigcap_{i=1}^{n} A_i\right)$ و $b - c \in \bigcap_{i=1}^{n} A_i$.

قضیهٔ باقیماندهٔ چینی از آنجهت این نام را یافته است که تعمیم مطلب زیر از نظریهٔ مقدماتی اعداداست که بر ریاضیدانان چینی سدهٔ اول بعد از میلاد معلوم بوده است .

نتیجهٔ ۲۶۰۲ . *فرض کنیم* $m_1, m_2, \ldots, m_n$ *اعداد صحیح مثبتی باشند به‌طوری که به‌ازای* $i \neq j$ ، $(m_i, m_j) = 1$. *هرگاه* $b_1, b_2, \ldots, b_n$ *اعداد صحیحی باشند ، آنگاه دستگاه همنهشتیهای*

$$x \equiv b_1 \,(mod\ m_1);\ x \equiv b_2 \,(mod\ m_2);\ \cdots;\ x \equiv b_n \,(mod\ m_n)$$

جواب صحیحی دارد که با تقریب به پیمانهٔ $m = m_1 m_2 \cdots m_n$ *به‌طورمنحصربه فرد معین می‌شود .*

طرح برهان . فرض کنیم $A_i = (m_i)$. پس $\bigcap_{i=1}^{n} A_i = (m)$. نشان دهید $(m_i, m_j) = 1$ ایجاب می‌کند که $A_i + A_j = \mathbf{Z}$ و قضیهٔ ۲۵۰۲ را به کار برید .

نتیجهٔ ۲۷۰۲ . *هرگاه* $A_1, \ldots, A_n$ *ایده‌آلهایی درحلقهٔ* R *باشند ، آنگاه یک تکریختی از حلقه‌ها مانند*

$$\theta : R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$$

وجود دارد . هرگاه به‌ازای هر i ، $R^2 + A_i = R$ ، *وبه‌ازای هر* $i \neq j$ ، $A_i + A_j = R$ ،

آنگاه θ یک یکریختی حلقه‌هاست.

طرح برهان. بنابر قضیهٔ ۲۳۰۲، برویختیهای کانونی

$$\pi_k : R \to R/A_k \ (k = 1, \ldots, n)$$

یک همریختی مانند $\theta_1 : R \to R/A_1 \times \cdots \times R/A_n$ از حلقه‌ها را القا می‌کند که $\theta_1(r) = (r + A_1, \ldots, r + A_n)$. واضح است که $\theta_1 = A_1 \cap \cdots \cap A_n$. بنابراین، θ_1 تکریختی $\theta : R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times \cdots \times R/A_n$ از حلقه‌ها را القا می‌کند (قضیهٔ ۹۰۲). نگاشت θ لزوماً سورژکتیو نیست (تمرین ۲۶). اما، هرگاه مفروضات قضیهٔ ۲۵۰۲ برقرار شده و $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$، آنگاه $b \in R$ ای وجود دارد به‌طوری که به‌ازای هر i، $b \equiv b_i \pmod{A_i}$. لذا،

$$\theta(b + \bigcap_i A_i) = (b + A_1, \ldots, b + A_n) = (b_1 + A_1, \ldots, b_n + A_n),$$

که از آنجا θ یک برویختی خواهد بود.

تمرینات

۱. مجموعهٔ تمام عناصر پوچ‌توان در یک حلقهٔ تعویضپذیر تشکیل یک ایده‌آل می‌دهند [ر.ک. تمرین ۱۲۰۱].

۲. فرض کنید I ایده‌آلی در حلقهٔ تعویضپذیر R بوده و

$$\operatorname{Rad} I = \{r \in R \mid r^n \in I \text{، به‌ازای } n \text{ ی}\}.$$

نشان دهید که $\operatorname{Rad} I$ یک ایده‌آل است.

۳. هرگاه R حلقه بوده و $a \in R$، آنگاه $J = \{r \in R \mid ra = 0\}$ یک ایده‌آل چپ و $K = \{r \in R \mid ar = 0\}$ یک ایده‌آل راست در R است.

۴. هرگاه I یک ایده‌آل چپ R باشد، آنگاه

$$A(I) = \{r \in R \mid rx = 0 \text{، به‌ازای هر } x \in I\}$$

یک ایده‌آل در R است.

۵. اگر I ایده‌آلی در حلقهٔ R باشد، قرار دهید

$$[R : I] = \{r \in R \mid xr \in I \text{، به‌ازای هر } x \in R\}$$

ثابت کنید $[R : I]$ ایده‌آلی از R است که شامل I می‌باشد.

۶. (آ) مرکز حلقهٔ تمام ماتریسهای 2×2 روی میدان F از همهٔ ماتریسها به شکل

$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ تشکیل شده است.

(ب) مرکز S ایده‌آلی در S نیست.

(پ) مرکز حلقهٔ تمام ماتریسهای $n \times n$ روی یک حلقهٔ بخشی چیست؟

۷. (آ) حلقهٔ یکدار R یک حلقهٔ بخشی است اگر و فقط اگر R ایده‌آل چپ حقیقی نداشته باشد. [حکم I ۳.۱۰ ممکن است مفید باشد.]

(ب) هرگاه S یک‌حلقه (احتمالا "بدون واحد") بدون ایده‌آل چپ حقیقی باشد، آنگاه یا $S^2 = 0$ یا S یک حلقهٔ بخشی است.

[**راهنمایی.** نشان دهید که $\{a \in S \mid Sa = 0\}$ یک ایده‌آل است. اگر $cd \neq 0$، نشان دهید که $\{r \in S \mid rd = 0\} = 0$. $e \in S$ را طوری بیابید که $ed = d$ و نشان دهید e یک واحد (دوطرفه) است.]

۸. فرض کنید R حلقه‌ای یکدار بوده و S حلقهٔ تمام ماتریسهای $n \times n$ روی R باشد. J یک ایده‌آل S است اگر و فقط اگر J حلقهٔ تمام ماتریسهای $n \times n$ روی ایده‌آلی در R مانند I باشد.

[**راهنمایی.** به‌ازای J داده‌شده، فرض کنید I مجموعهٔ تمام عناصری از R باشد که به‌صورت درایهٔ سطر 1 ــ ستون 1 ماتریسی در J ظاهر می‌شوند. از ماتریسهای $E_{r,s}$، که $1 \leq r \leq n$, $1 \leq s \leq n$، و اینکه $E_{r,s}$ دارای 1_R به عنوان درایهٔ سطر r ــ ستون s و 0 در جاهای دیگر است استفاده کنید. توجه کنید که، به‌ازای ماتریس $A = (a_{ij})$، $E_{p,r}AE_{s,q}$ ماتریسی است با درایهٔ a_{rs} در سطر p ــ ستون q و 0 در جاهای دیگر.]

۹. فرض کنید S حلقهٔ تمام ماتریسهای $n \times n$ روی حلقهٔ بخشی D باشد.

(آ) S ایده‌آل حقیقی ندارد (یعنی، 0 یک ایده‌آل ماکزیمال است).

[**راهنمایی.** تمرین ۸ را به کار برید یا، با استفاده از ماتریسهای $E_{r,s}$ مذکور در آنجا، مستقیما" استدلال کنید.]

(ب) S مقسوم‌علیه صفر دارد. درنتیجه، (یک) $S \ncong S/0$ یک حلقهٔ بخشی نیست و (دو) 0 یک‌ایده‌آل‌اول‌است‌که‌درشرط (۱) قضیهٔ ۱۵.۲ صدق‌نمی‌کند.

۱۰. (آ) نشان دهید $\mathbf{Z}$ یک حلقهٔ ایده‌آل اصلی است [ر.ک. قضیهٔ I ۱.۳۰].

(ب) هر نقش همریخت یک حلقهٔ ایده‌آل‌اصلی نیز یک حلقهٔ ایده‌آل اصلی است.

(پ) Z_m به‌ازای هر $m > 0$ یک حلقهٔ ایده‌آل اصلی است.

۱۱. هرگاه N ایده‌آل تمام عناصر پوچ‌توان در حلقهٔ تعویضپذیر R باشد (ر.ک. تمرین ۱)، آنگاه حلقهٔ R/N هیچ عنصر پوچ‌توان ناصفر ندارد.

۱۲. فرض کنید R حلقه‌ای بدون واحد و مقسوم‌علیه صفر باشد. همچنین، S حلقه‌ای باشد که گروه جمعی آن مثل برهان قضیهٔ ۱۰.۱۰ مساوی $R \times \mathbf{Z}$ است. فرض کنید

$$A = \{(r,n) \in S \mid rx + nx = 0 \text{ ، به‌ازای هر } x \in R\}.$$

(آ) A یک ایده‌آل در S است.

(ب) S/A یکدار بوده و شامل زیرحلقه‌ای یکریخت با R است.

(پ) S/A مقسوم‌علیه صفر ندارد.

۱۳. فرض کنید $f : R \to S$ یک همریختی حلقه‌ها بوده، I ایده‌آلی در R، و J ایده‌آلی در S باشد.

(آ) $f^{-1}(J)$ ایده‌آلی در R است که شامل $\operatorname{Ker} f$ می‌باشد.

(ب) هرگاه f یک بروریختی باشد، آنگاه $f(I)$ ایده‌آلی در S است. اگر f سورژکتیو نباشد، $f(I)$ لزوماً ایده‌آلی در S نیست.

۱۴. هرگاه P ایده‌آلی در حلقهٔ R باشد که لزوماً تعویضپذیر نیست، آنگاه شرایط زیر معادلند.

(آ) P یک ایده‌آل اول است.

(ب) هرگاه $r,s \in R$ چنان باشند که $rRs \subset P$، آنگاه $r \in P$ یا $s \in P$.

[**راهنمایی.** هرگاه (آ) برقرار بوده و $rRs \subset P$، آنگاه $(RrR)(RsR) \subset P$، که از آنجا $RrR \subset P$ یا $RsR \subset P$؛ مثلاً، $RrR \subset P$. هرگاه $A = (r)$، آنگاه $A^3 \subset RrR \subset P$، که از آنجا $r \in A \subset P$.]

(پ) هرگاه (r) و (s) ایده‌آلهای اصلی R باشند به‌طوری‌که $(r)(s) \subset P$، آنگاه $r \in P$ یا $s \in P$.

(ت) هرگاه U و V ایده‌آلهایی راست در R باشند به‌طوری‌که $UV \subset P$، آنگاه $U \subset P$ یا $V \subset P$.

(ث) هرگاه U و V ایده‌آلهایی چپ در R باشند به‌طوری که $UV \subset P$، آنگاه $U \subset P$ یا $V \subset P$.

۱۵. مجموعهٔ مرکب از صفر و تمام مقسوم‌علیه‌های صفر حلقه‌ای تعویضپذیر و یکدار

دست‌کم شامل یک ایده‌آل اول است.

۱۶. فرض کنید R حلقه‌ای تعویضپذیر و یکدار بوده و ایده‌آل A از R مشمول اجتماعی متناهی‌مانند $P_1 \cup \cdots \cup P_n$ از ایده‌آلهای اول باشد. نشان دهید که به‌ازای i ی، $A \subset P_i$.

[**راهنمایی.** درغیراین‌صورت، می‌توان فرض کرد به‌ازای هر j، $A \cap P_j \not\subset \bigcup_{i \neq j} P_i$. فرض کنید $a_j \in (A \cap P_j) - (\bigcup_{i \neq j} P_i)$. در این صورت، $a_1 + a_2 a_3 \cdots a_n$ در A است ولی در $P_1 \cup \cdots \cup P_n$ نیست.]

۱۷. فرض کنید $f : R \to S$ یک برووریختی حلقه‌ها با هستهٔ K باشد.

(آ) هرگاه P یک ایده‌آل اول در R و شامل K باشد، آنگاه $f(P)$ یک ایده‌آل اول در S است [ر.ک. تمرین ۱۳].

(ب) هرگاه Q ایده‌آل اولی در S باشد، آنگاه $f^{-1}(Q)$ ایده‌آل اولی در R است که شامل K می‌باشد.

(پ) تناظر یک به یکی بین مجموعهٔ تمام ایده‌آلهای اول در R که شامل K اندو مجموعهٔ تمام ایده‌آلهای اول در S وجود دارد که با $P \mapsto f(P)$ نموده می‌شود.

(ت) هرگاه I ایده‌آلی درحلقهٔ R باشد، آنگاه هر ایده‌آل اول در R/I به شکل P/I است، که در آن P ایده‌آل اولی در R شامل I است.

۱۸. ایده‌آل $M \neq R$ درحلقهٔ تعویضپذیر و یکدار R ماکزیمال است اگر و فقط اگر به‌ازای هر $r \in R - M$، $x \in R$ ی وجود دارد به‌طوری‌که $1_R - rx \in M$.

۱۹. حلقهٔ E از اعداد صحیح زوج شامل ایده‌آل ماکزیمالی مانند M است به‌طوری‌که E/M میدان نیست.

۲۰. در حلقهٔ Z، شرایط‌زیر بر ایده‌آل ناصفر I معادلند:

(یک) I اول است؛ (دو) I ماکزیمال است؛ (سه) $I = (p)$ که در آن p اول است.

۲۱. تمام ایده‌آلهای اول و ماکزیمال در حلقهٔ Z_m را تعیین کنید.

۲۲. (آ) هرگاه $R_1, \ldots, R_n$ حلقه‌های یکداری بوده و I ایده‌آلی در $R_1 \times \cdots \times R_n$ باشد، آنگاه $I = A_1 \times \cdots \times A_n$، که در آن هر A_i ایده‌آلی در R_i است.

[**راهنمایی.** با معلوم بودن I، فرض کنید $A_k = \pi_k(I)$، که در آن $\pi_k : R_1 \times \cdots \times R_n \to R_k$ برووریختی کانونی است.]

(ب) نشان دهید که اگر حلقه‌های R_i یکدار نباشند، نتیجهٔ (آ) لزوماً برقرار نیست.

۲۳. عنصر e در حلقهٔ R را **خودتوان** گوییم اگر $e^2 = e$. یک عنصر از مرکز حلقهٔ R را **مرکزی** می‌نامیم. هرگاه e یک خودتوان مرکزی در حلقهٔ یکدار R باشد، آنگاه

(آ) $1_R - e$ یک خودتوان مرکزی است؛

(ب) eR و $(1_R - e)R$ ایده‌آلهایی در R اند به‌طوری‌که

$$R = eR \times (1_R - e)R.$$

۲۴. عناصر خودتوان $e_1, \ldots, e_n$ در حلقهٔ R [ر.ک. تمرین ۲۳] را **متعامد** گوییم اگر به‌ازای $i \neq j$، $e_ie_j = 0$. هرگاه $R, R_1, \ldots, R_n$ حلقه‌های یکداری باشند، آنگاه شرایط زیر معادلند:

(آ) $R \cong R_1 \times \cdots \times R_n$.

(ب) R شامل مجموعه‌ای مانند $\{e_1, \ldots, e_n\}$ از خودتوانهای مرکزی متعامد [تمرین ۲۳] است که $e_1 + e_2 + \cdots + e_n = 1_R$ و به‌ازای هر i، $e_iR \cong R_i$.

(پ) R حاصلضرب مستقیم داخلی $R = A_1 \times \cdots \times A_n$ است، که در آن هر A_i یک ایده‌آل R است به‌طوری‌که $A_i \cong R_i$.

[**راهنمایی.** (ب) $\Rightarrow$ (آ) عناصر

$$\bar{e}_1 = (1_{R_1}, 0, \ldots, 0),\ \bar{e}_2 = (0, 1_{R_2}, 0, \ldots, 0), \ldots, \bar{e}_n = (0, \ldots, 0, 1_{R_n})$$

خودتوانهای مرکزی متعامد در $S = R_1 \times \cdots \times R_n$ اند به‌طوری‌که $\bar{e}_1 + \cdots + \bar{e}_n = 1_S$ و $\bar{e}_iS \cong R_i$.

(پ) $\Rightarrow$ (ب) توجه کنید که $A_k = e_kR$ ایده‌آل اصلی (e_k) در R است و e_iR خود حلقه‌ای با واحد e_k است.]

۲۵. هرگاه $m \in \mathbf{Z}$ تجزیهٔ اولی مانند $m = p_1^{k_1} \cdots p_t^{k_t}$ ($k_i > 0$؛ p_i ها اعداد اول متمایزی هستند) داشته باشد، آنگاه یک یکریختی از حلقه‌ها مانند $Z_m \cong Z_{p_1^{k_1}} \times \cdots \times Z_{p_t^{k_t}}$ وجود دارد. [**راهنمایی.** نتیجهٔ ۲۷۰۲.]

۲۶. هرگاه $R = \mathbf{Z}$، $A_1 = (6)$، و $A_2 = (4)$، آنگاه نگاشت $\theta : R/A_1 \cap A_2 \to R/A_1 \times R/A_2$ نتیجهٔ ۲۷۰۲ سورژکتیو نیست.

۳ تجزیه در حلقه‌های تعویضپذیر

در این بخش مفاهیم بخشپذیری، بزرگترین مقسوم علیه مشترک، و اول بودن در حلقهٔ

اعداد صحیح را به حلقه‌های تعویضپذیر دلخواه تعمیم داده و آن دامنه‌های صحیح را بررسی می‌کنیم که در آنها مشابه قضیهٔ اساسی حساب (آشنایی، قضیهٔ ۷.۶) برقرار است. نتیجهٔ مهم این است که هر دامنهٔ ایده‌آل اصلی یک دامنهٔ تجزیهٔ یکتاست. به علاوه، آن حلقه‌های تعویضپذیری را مطالعه می‌کنیم که در آنها مشابه الگوریتم تقسیم برقرارباشد (حلقه‌های اقلیدسی).

تعریف ۱.۳. گوییم عنصر ناصفر a از حلقهٔ تعویضپذیر R عنصر $b \in R$ را ***عاد می‌کند*** (نماد: $a \mid b$) اگر $x \in R$ ی موجود باشد به‌طوری‌که $ax = b$. گوییم عناصر a,b از R ***شریک‌اند*** اگر $a \mid b$ و $b \mid a$.

همانطورکه اینک خواهیم دید، اساساً تمام احکام مربوط به بخشپذیری را می‌توان برحسب ایده‌آلهای اصلی بیان کرد.

قضیهٔ ۲.۳. *فرض کنیم* a، b، و u *عناصری از حلقهٔ تعویضپذیر و یکدار* R *باشند.*

(یک) $a \mid b$ *اگر و فقط اگر* $(b) \subset (a)$.

(دو) a و b *شریک‌اند اگر و فقط اگر* $(a) = (b)$.

(سه) u *یکه است اگر و فقط اگر به‌ازای هر* $r \in R$، $u \mid r$.

(چهار) u *یکه است اگر و فقط اگر* $(u) = R$.

(پنج) *رابطهٔ "* a *شریک* b *است" یک رابطهٔ هم‌ارزی بر* R *است.*

(شش) *هرگاه* $a = br$ *که در آن* $r \in R$ *یکه است، آنگاه* a و b *شریک‌اند. اگر* R *دامنهٔ صحیح باشد، عکس این نیز درست است.*

برهان. تمرین؛ قضیهٔ ۵.۲ (پنج) ممکن است برای (یک) و (دو) مفید باشد.

تعریف ۳.۳. فرض کنیم R حلقهٔ تعویضپذیر و یکدار باشد. عنصر c از R ***تحویل‌ناپذیر*** است مشروط بر اینکه

(یک) c یک غیر یکهٔ ناصفر باشد؛

(دو) $c = ab \Rightarrow$ a یا b یکه است.

عنصر p از R *اول* است مشروط بر اینکه
(یک) p یک غیر یکهٔ ناصفر باشد؛
(دو) $p|a$ یا $p|b \Rightarrow p|ab$.

چند مثال. هرگاه p یک عدد صحیح اول معمولی باشد، آنگاه هردوی p و $-p$ در $\mathbf{Z}$ به معنی تعریف ۳۰۳ تحویل‌ناپذیر و اولند. در حلقهٔ Z_6، به آسانی معلوم می‌شود که 2 اول است. اما $2 \in Z_6$ تحویل‌ناپذیر نیست، زیرا $2 = 2 \cdot 4$ و هیچیک از 2 و 4 در Z_6 یکه نیست (درواقع، اینها مقسوم‌علیه‌های صفرند). برای مثالی از یک عنصر تحویل‌ناپذیر که اول نیست، ر.ک. تمرین ۳.

بین عناصر اول [تحویل‌ناپذیر] در حلقهٔ R و ایده‌آلهای اصلی اول [ماکزیمال] در R رابطهٔ نزدیکی وجود دارد.

قضیهٔ ۴۰۳. *فرض کنیم* p و c *عناصر ناصفری در دامنهٔ صحیح* R *باشند.*
(یک) p *اول است اگر و فقط اگر* (p) *ایده‌آل اول ناصفر باشد.*
(دو) c *تحویل‌ناپذیر است اگر و فقط اگر* (c) *در مجموعهٔ* S *مرکب از تمام ایده‌آلهای اصلی حقیقی* R *ماکزیمال باشد.*
(سه) *هر عنصر اول* R *تحویل‌ناپذیر است.*
(چهار) *هرگاه* R *یک دامنهٔ ایده‌آل اصلی باشد، آنگاه* p *اول است اگر و فقط اگر* p *تحویل‌ناپذیر باشد.*
(پنج) *هر شریک یک عنصر تحویل‌ناپذیر [اول]* R *تحویل‌ناپذیر [اول] است.*
(شش) *تنها مقسوم‌علیه‌های یک عنصر تحویل‌ناپذیر* R *شریکهای آن و یکه‌های* R *می‌باشند.*

تبصره. همانطور که در برهان زیر می‌بینیم، بعضی از قسمتهای قضیهٔ ۴۰۳ برای یک حلقهٔ تعویضپذیر یکدار درست است.

***طرح برهان* ۴۰۳.** (یک) از تعریف ۳۰۳ وقضیهٔ ۱۵۰۲ استفاده کنید. (دو) هرگاه c تحویل‌ناپذیر باشد، آنگاه، طبق قضیهٔ ۲۰۳، (c) یک ایده‌آل حقیقی R است.

هرگاه $(c) \subset (d)$ ، آنگاه $c = dx$. چون c تحویل‌ناپذیر است، یا d یکه است (که از آنجا $(d) = R$) یا x یکه است (که از آنجا، طبق قضیهٔ ۲۰۳ ، $(c) = (d)$) . از اینرو، (c) در S ماکزیمال است. بـه عکس، هـرگاه (c) در S ماکزیمال باشد، آنگاه، طبق قضیهٔ ۲۰۳ ، c یک غیر یکهٔ (ناصفر) در R است. هرگاه $c = ab$ ، آنگاه $(c) \subset (a)$ ، که از آنجا $(a) = (c)$ یا $(a) = R$. هرگاه $(a) = R$ ، آنگاه a یکه‌است (قضیهٔ ۲۰۳) . هرگاه $(a) = (c)$ ، آنگاه $a = cy$ ؛ و درنتیجه، $c = ab = cyb$. چـون R یـک دامنهٔ صحیح است، داریم $yb = 1$ ، درنتیجه b یکه است. بنابراین، c تحویل‌ناپذیر است.

(سه) هرگاه $p = ab$ ، آنگاه $p \mid a$ یا $p \mid b$ ؛ مثلاً " $p \mid a$. در این صورت، $px = a$ و $p = ab = pxb$ ، که رابطهٔ $xb = 1$ را ایجاب مـی‌کند. بنابراین، b یکه می‌باشد.

(چهار) اگر p تحویل‌ناپذیر باشد، با استفاده از قسمت (دو)، قضیهٔ ۱۹۰۲ ، و قسمت (یک) نشان دهید که p اول است. (پنج) هرگاه c تحویل‌ناپذیر و d یک شریک c باشد، آنگاه $c = du$ که در آن $u \in R$ یکه اسـت (قضیهٔ ۲۰۳) . هرگاه $d = ab$ ، آنگاه $c = abu$ ، که‌ازآنجا a یا bu یکه است. اما اگر bu یکه باشد، b نیز یکه است. ازاینرو d تحویل‌ناپذیراست. (شش) هرگاه c تحویل‌ناپذیربوده‌و $a \mid c$ ، آنگاه $(c) \subset (a)$ ، که از آنجا، بنابر (دو)، $(a) = (c)$ یا $(a) = R$. بنابراین، طبق قضیهٔ ۲۰۳ ، a یک شریک c است یا یکه می‌باشد.

حال مفاهیم مشـابه بخشپذیری و اعداد صحیح اول در حلقهٔ $\mathbf{Z}$ را در یک دامنهٔ صحیح دلخـواه عـرضه می‌کنیم. به یاد آورید که، بنابرقضیهٔ اساسی حساب (آشنایی، قضیهٔ ۷۰۶)، هـر عنصر در $\mathbf{Z}$ حاصلضربی از تعدادی متناهی از عناصر تحویل‌ناپذیر (اعداد صحیح اول یا قرینه‌های آنها) است. به علاوه، این تجزیه (جز در مورد ترتیب عوامل تحویل‌ناپذیر) منحصر به فرد است. درنتیجه، $\mathbf{Z}$ مثالی است از:

تعریف ۵۰۳ . دامنهٔ صحیح R یک **دامنهٔ یکتایی تجزیه** است مشروط بر اینکه

(یک) هر عنصر غیر یکهٔ ناصفر a از R را بتوان به صورت $a = c_1c_2\cdots c_n$ نوشت، که در آن $c_1, \ldots, c_n$ تحویل‌ناپذیر است.

(دو) هرگاه $a = c_1c_2\cdots c_n$ و $a = d_1d_2\cdots d_m$ (c_i, d_i ها تحویل‌نـاپذیرند) ، آنـگاه، $n = m$ و به‌ازای‌جایگشتی‌مانند σ از $\{1,2,\ldots,n\}$ ، به‌ازای‌هر i ، c_i و $d_{\sigma(i)}$ شریک‌اند.

تبصره. بنابر قسمت (دو) هر عنصر تحویل‌ناپذیر در یک دامنهٔ یکتایی تجزیه لزوما " اول است. درنتیجه، بنابر قضیهٔ ۴۰۳ (سه)، عناصر تحویل‌ناپذیر و اول یکی خواهند بود.

تعریف ۵۰۳ نـابدیهی است بدین معنی که دامنه‌های صحیحی وجود دارند که در آنها هر عنصر حاصل ضربی متناهی از عناصر تحویل‌ناپذیر است، اما این تجزیه منحصر به‌فرد نیست (یعنی، تعـریف ۵۰۳ (دو) برقرار نیست)؛ ر.ک. تمرین ۴. درواقع، یکی از دلایل تاریخی برای معرفی مفهوم **ایده‌آل** این بوده است که در حلقه‌های اعداد صحیح جبری که‌تجزیهٔ‌عناصرلزوما "منحصر به فردنیست، نوعی از قضایای یکتایی تجزیه‌را (برای ایده‌آلها) به دست آوریم؛ ر.ک. فصل هشت.

با ملاحظهٔ ارتباط عناصر تحویل‌ناپذیر و ایده‌آلهای اصلی (قضیهٔ ۴۰۳) و مثال در مورداعدادصحیح، موجه‌به نظر می‌رسد که هر دامنهٔ ایده‌آل اصلی یک دامنهٔ یکتایی تجزیه باشد. برای اثبات این امر، به لم زیر نیاز داریم.

لم ۶۰۳. *هرگاه* R *یک‌حلقهٔ‌ایده‌آل‌اصلی بوده و* $(a_1) \subset (a_2) \subset \cdots$ *زنجیری از ایده‌آلها در* R *باشد، آنگاه، به‌ازای‌عدد‌صحیح مثبتی چون* n *و به‌ازای هر* $j \geq n$ ، $(a_j) = (a_n)$.

برهان. فرض‌کنیم $A = \bigcup_{i \geq 1} (a_i)$. حکم می‌کنیم که A ایده‌آل است. هرگاه $b,c \in A$، آنگاه $b \in (a_i)$ و $c \in (a_j)$. درنتیجه، $i \leq j$ یا $j \leq i$؛ مثـلا "، $i \geq j$. و $(a_i) \subset (a_j)$ $b,c \in (a_j)$. چون (a_i) ایده‌آل است، $b - c \in (a_j) \subset A$. به همین نحو، هرگاه $r \in R$ و $b \in A$، آنگاه $b \in (a_i)$، که از آنجا $rb \in (a_i) \subset A$ و $br \in (a_i) \subset A$. بنـابراین، طبق قضیـهٔ ۲۰۲، A ایده‌آل اسـت. طبق فرض، A اصلی است؛ مثلا "، $A = (a)$. چون $a \in A = \bigcup (a_i)$، به‌ازای n ی، $a \in (a_n)$. طبق تعریف ۴۰۲، $(a) \subset (a_n)$. بنابراین، به‌ازای هر $j \geq n$، $(a) \subset (a_n) \subset (a_j) \subset A = (a)$، که از آنجا $(a_j) = (a_n)$.

قضیهٔ ۷۰۳. *هر دامنهٔ ایده‌آل اصلی* R *یک دامنهٔ یکتایی تجزیه است.*

تبصره. عکس قضیهٔ ۷۰۳ درست‌نیست. مثلا "، می‌توان‌نشان داد که حلقهٔ چندجمله‌ای

$\mathbf{Z}[x]$ یک دامنهٔ یکتایی تجزیه است (قضیهٔ ۱۴۰۶ در زیر)، ولی $\mathbf{Z}[x]$ یک دامنه ایده‌آل اصلی نیست (تمرین ۱۰۶).

طرح برهان ۷۰۳. فرض کنیم S مجموعهٔ تمام عناصر غیر یکهٔ ناصفر R باشد که نمی‌توان آنها را به صورت حاصلضربی متناهی از عناصر تحویل‌ناپذیر تجزیه کرد. ابتدا نشان می‌دهیم که S تهی است، که از آنجا نتیجه می‌شود که هر عنصر غیر یکهٔ ناصفر R حداقل یک تجزیه به صورت حاصلضربی متناهی از عناصر تحویل‌ناپذیر دارد. فرض کنیم S تهی نبوده و $a \in S$. در این صورت، طبق قضیهٔ ۲۰۳ (چهار)، (a) یک ایده‌آل حقیقی است و، بنابر قضیهٔ ۱۸۰۲، مشمول یک ایده‌آل ماکزیمال مانند (c) است. بنابر قضیهٔ ۴۰۳ (دو)، $c \in R$ تحویل‌ناپذیر است. چون $(a) \subset (c)$، c، a را عاد می‌کند. بنابراین، می‌توان به‌ازای هر $a \in S$ یک مقسوم علیه تحویل‌ناپذیر c_a از a را انتخاب کرد (اصل انتخاب). چون R یک دامنهٔ صحیح است، c_a عنصر ناصفر $x_a \in R$ با خاصیت $c_a x_a = a$ را به‌طور منحصر به فرد معین می‌کند. حکم می‌کنیم که $x_a \in S$. زیرا هرگاه x_a یکه می‌بود، آنگاه $a = c_a x_a$ طبق قضایای ۲۰۳ (شش) و ۴۰۳ (پنج) تحویل‌ناپذیر می‌شد. هرگاه x_a غیر یکه بوده و در S نباشد. آنگاه x_a تجزیه‌ای به‌صورت حاصلضرب عناصری تحویل ناپذیر دارد؛ که در نتیجه، a نیز چنین است. چون $a \in S$، این یک تناقض است. از اینرو، $x_a \in S$. به‌علاوه، حکم می‌کنیم که ایده‌آل (a) حقیقتاً مشمول ایده‌آل (x_a) است. چون $x_a \mid a$، طبق قضیهٔ ۲۰۳ (یک)، $(a) \subset (x_a)$. اما $(a) = (x_a)$ ایجاب می‌کند که به‌ازای $y \in R$ ی، $a = x_a c_a = a y c_a$ که از آنجا $x_a = a y$ و درنتیجه $y c_a = 1$. این با تحویل‌ناپذیری c_a (و درنتیجه، غیر یکه بودن آن) تعارض دارد. بنابراین، $(a) \subsetneq (x_a)$.

نکات فوق نشان می‌دهند که تابع $f : S \to S$ داده شده با $f(a) = x_a$ تعریف شده است. بنابر قضیهٔ بازگشتی ۲۰۶ آشنایی (با فرض $f = f_n$ به‌ازای هر n)، تابعی مانند $\varphi : \mathbf{N} \to S$ وجود دارد به‌طوری که

$$\varphi(0) = a \quad \text{و} \quad \varphi(n+1) = f(\varphi(n)) = x_{\varphi(n)} \ (n \geq 0).$$

اگر $\varphi(n)$ را با a_n نشان دهیم، دنباله‌ای از عناصر S خواهیم داشت: $a, a_1, a_2, \ldots$ به طوری‌که

$$a_1 = x_a;\ a_2 = x_{a_1};\ \cdots;\ a_{n+1} = x_{a_n};\ \cdots.$$

درنتیجه، بند فوق نشان می‌دهد که یک زنجیر افزایشی از ایده‌آلها مانند

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots$$

وجود دارد، کـه بـا لم ۶.۳ در تضاد است. بنابراین، مجموعهٔ S باید تهی باشد؛ درنتیجه، هر عنصر غیر یکهٔ ناصفر در R تجزیه‌ای به صورت یک حاصلضرب متناهی از تحویل‌ناپذیرها دارد.

بالاخره، هرگاه $c_1c_2\cdots c_n = a = d_1d_2\cdots d_m$ (c_i, d_i ها تحـویل‌ناپذیرند)، آنگاه، بنابر قضیهٔ ۴.۳ (چهار)، c_1 ، d_i ی را عـاد می‌کند. چون c_1 غیر یکه است، بنابر قضیهٔ ۴.۳ (شش)، باید یک شریک d_i باشد. حال می‌توان اثبات یکتایی را با استدلال استقرایی عادی تمام کرد.

چند دامنـهٔ صحیح مهم که مکرر به آنـها برمی‌خوریم خواصی دارند که دامنه‌های صحیح دیگر از آنها بهره ندارند.

تعریف ۸.۳. فرض کنیم $\mathbf{N}$ مجموعهٔ اعداد صحیح نامنفی بوده و $\mathbf{R}$ حلقه‌ای تعویضپذیر باشد. $\mathbf{R}$ یک ***حلقهٔ اقلیدسی*** است اگر تابعی مانند $\varphi : \mathbf{R} - \{0\} \to \mathbf{N}$ وجود داشته باشد به‌طوری که

(یک) هرگاه $a,b \in \mathbf{R}$ و $ab \neq 0$، آنگاه $\varphi(a) \leq \varphi(ab)$؛

(دو) هرگاه $a,b \in \mathbf{R}$ و $b \neq 0$، آنگاه $q,r \in \mathbf{R}$ ی وجود دارنـد به‌طوری‌که $a = qb + r$ که در آن $r = 0$، یا $r \neq 0$ و $\varphi(r) < \varphi(b)$.

هر حلقهٔ اقلیدسی که دامنهٔ صحیح نیز باشد یک ***دامنهٔ اقلیدسی*** نام دارد.

مثال. حلقهٔ $\mathbf{Z}$ اعداد صحیح با $\varphi(x) = |x|$ یک دامنهٔ اقلیدسی است.

مثال. اگر F میدان بـاشد، به‌ازای هر $x \in F$ که $x \neq 0$، قرار می‌دهیم $\varphi(x) = 1$. در این صورت، F یک دامنهٔ اقلیدسی است.

مثال. هرگاه F میدان باشد، آنگاه حلقهٔ چندجمله‌ایهای یک متغیرهٔ $F[x]$ یک دامنهٔ

اقلیدسی با درجهٔ f $\varphi(f) =$ است؛ ر.ک. نتیجهٔ ۴.۶ در زیر.

مثال. فرض کنیم $\mathbf{Z}[i]$ زیرمجموعهٔ $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ از اعداد مختلط باشد. $\mathbf{Z}[i]$ یک دامنهٔ صحیح است که دامنهٔ ***اعداد صحیح گاوسی*** نام دارد.
تعریف می‌کنیم $\varphi(a + bi) = a^2 + b^2$. واضح است که اگر $a + bi \neq 0$، $\varphi(a + bi) \neq 0$؛ همچنین، به آسانی می‌توان نشان داد که شرط (یک) تعریف برقرار است. اثبات صدق کردن φ در شرط (دو) را به خواننده محول می‌کنیم (تمرین ۶).

قضیهٔ ۹.۳. ***هر حلقهٔ اقلیدسی R یک حلقهٔ ایده‌آل اصلی یکدار است. درنتیجه، هر دامنهٔ اقلیدسی یک دامنهٔ یکتایی تجزیه است.***

تبصره. عکس قضیهٔ ۹.۳ درست نیست، زیرا دامنه‌های ایده‌آل اصلیی وجود دارند که دامنهٔ اقلیدسی نیستند (تمرین ۸).

برهان ۹.۳. اگر I ایده‌آل ناصفری در R باشد، $a \in I$ را طوری می‌گیریم که $\varphi(a)$ کوچکترین عدد صحیح در مجموعهٔ اعداد صحیح نامنفی $\{\varphi(x) \mid x \neq 0;\ x \in I\}$ باشد. هرگاه $b \in I$، آنگاه $b = qa + r$ که‌درآن $r = 0$ یا $r \neq 0$ و $\varphi(r) < \varphi(a)$. چون $b \in I$ و $qa \in I$، r لزوماً در I است. چون $\varphi(r) < \varphi(a)$ انتخاب a را نقض می‌کند، باید داشته باشیم $r = 0$، که از آنجا $b = qa$. درنتیجه، طبق قضیهٔ ۵.۲، $I \subset Ra \subset (a) \subset I$. بنابراین، $I = Ra = (a)$ و R یک حلقهٔ ایده‌آل اصلی است.

چون R خود ایده‌آل است، به‌ازای $a \in R$ ای، $R = Ra$. درنتیجه، به‌ازای $e \in R$ ای، $a = ea = ae$. هرگاه $b \in R = Ra$، آنگاه به‌ازای $x \in R$ ی، $b = xa$. بنابراین، $be = (xa)e = x(ae) = xa = b$؛ درنتیجه، e یک عنصر همانی ضربی برای R است. حال قسمت آخر قضیه نتیجهٔ فوری قضیهٔ ۷.۳ می‌باشد.

این بخش را با چند نکتهٔ دیگر در باب بخشپذیری که گهگاه در آینده به کار می‌روند (بخشهای ۵، ۶، و IV ۶.۰) پایان می‌بخشیم.

تعریف ۱۰.۳. فرض کنیم X زیرمجموعه‌ای ناتهی از حلقهٔ تعویضپذیر R باشد. عنصر

$d \in R$ **بزرگترین مقسوم‌علیه مشترک** X است مشروط بر اینکه
(یک) به‌ازای هر $a \in X$ ، $d \mid a$ ؛
(دو) $c \mid d \Rightarrow$ به‌ازای هر $a \in X$ ، $c \mid a$.

بزرگترین مقسوم‌علیه‌های مشترک همیشه وجود ندارند . مثلا" ، در حلقهٔ اعداد صحیح زوج E ، 2 مقسوم‌علیه‌ندارد ؛ درنتیجه ، 2 و 4 (بزرگترین) مقسوم‌علیه مشترک ندارند . حتی وقتی بزرگترین مقسوم‌علیه مشترک $a_1, \ldots, a_n$ موجود است ، لازم نیست منحصر به فرد باشد . اما ، طبق (دو) ، واضح است که هر دو بزرگترین مقسوم‌علیه مشترک X شریک‌اند . به‌علاوه ، به‌آسانی می‌بینیم که هر شریک یک بزرگترین مقسوم‌علیه مشترک X یک بزرگترین مقسوم‌علیه‌مشترک X است . هرگاه R یکدار بوده و $a_1, a_2, \ldots, a_n$ دارای بزرگترین مقسوم‌علیه مشترک 1_R باشند ، آنگاه گوییم $a_1, a_2, \ldots a_n$ **نسبت به هم اول‌اند** .

قضیهٔ ۱۱.۳ . فرض کنیم $a_1, \ldots, a_n$ **عناصری از حلقهٔ تعویضپذیر و یکدار** R **باشند .**
(یک) $d \in R$ **بزرگترین مقسوم‌علیه مشترکی از** $\{a_1, \ldots, a_n\}$ **است به‌طوری که به‌ازای** $r_i \in R$ **هایی ،** $d = r_1a_1 + \cdots + r_na_n$ **اگر و فقط اگر** $(d) = (a_1) + (a_2) + \cdots + (a_n)$.
(دو) هرگاه R **یک حلقهٔ ایده‌آل اصلی باشد ، آنگاه بزرگترین مقسوم‌علیه مشترکی از** $a_1, \ldots, a_n$ **موجود بوده و هر یک به شکل** $r_1a_1 + \cdots + r_na_n$ $(r_i \in R)$ **می‌باشد .**
(سه) هرگاه R **دامنهٔ یکتایی تجزیه باشد ، آنگاه بزرگترین مقسوم‌علیه مشترکی از** $a_1, \ldots, a_n$ **وجود دارد .**

تبصره . قضیهٔ ۱۱.۳ (یک) نمی‌گوید که هر بزرگترین مقسوم‌علیه مشترک $a_1, \ldots, a_n$ ترکیبی خطی از $a_1, \ldots, a_n$ است . این به‌طورکلی درست نیست (تمرین ۱۵.۶) . همچنین ، ر.ک. تمرین ۱۲ .

طرح برهان ۱۱.۳ . (یک) از تعریف ۱.۳ و قضیهٔ ۵.۲ استفاده کنید . قسمت (دو) از قسمت (یک) نتیجه‌می‌شود . (سه) هر a_i دارای تجزیه‌ای به صورت $a_i = c_1^{m_{i1}} c_2^{m_{i2}} \cdots c_t^{m_{it}}$ است ، که در آن $c_1, \ldots, c_t$ عناصر تحویل‌ناپذیر متمایزی هستند و هر $m_{ij} \geq 0$. نشان دهید که $d = c_1^{k_1} c_2^{k_2} \cdots c_t^{k_t}$ بزرگترین مقسوم‌علیه مشترک $a_1, \ldots, a_n$ است ، که در آن

$\cdot\ k_j = \min\{m_{1j}, m_{2j}, m_{3j}, \ldots, m_{nj}\}$

تمرینات

۱ . هر ایده‌آل ناصفر دریک دامنهٔ ایده‌آل اصلی ماکزیمال است اگر و فقط اگر اول باشد .

۲ . دامنهٔ صحیح R دامنهٔ یکتایی تجزیه است اگر و فقط اگر هر ایده‌آل اول ناصفر در R شامل ایده‌آل اصلی ناصفری است که اول می‌باشد .

۳ . فرض کنید R زیر حلقهٔ $\{a + b\sqrt{10} \mid a,b \in \mathbf{Z}\}$ از میدان اعداد حقیقی باشد .

(آ) نگاشت $N : R \to \mathbf{Z}$ داده شده با

$$a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$$

چنان است که به‌ازای هر $u,v \in R$ ، $N(uv) = N(u)N(v)$ و $N(u) = 0$ اگر و فقط اگر $u = 0$.

(ب) u در R یکه است اگر و فقط اگر $N(u) = \pm 1$.

(پ) 2 ، 3 ، $4 + \sqrt{10}$ ، و $4 - \sqrt{10}$ عناصر تحویل‌ناپذیری از R اند .

(ت) 2 ، 3 ، $4 + \sqrt{10}$ ، و $4 - \sqrt{10}$ عناصر اولی از R نیستند .

[**راهنمایی** . $(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 3 \cdot 2$]

۴ . نشان دهید که در دامنهٔ صحیح تمرین ۳ ، هر عنصر را می‌توان به حاصلضربی از عناصر تحویل‌ناپذیر تجزیه کرد ، ولی این تجزیه لازم نیست (به معنی تعریف ۵۰۳ (دو)) منحصر به فرد باشد .

۵ . فرض کنید R یک دامنهٔ ایده‌آل اصلی باشد .

(آ) هرایده‌آل‌حقیقی حاصلضربی ازایده‌آلهای ماکزیمال مانند $P_1P_2 \cdots P_n$ است ، که صرف‌نظر از ترتیب به‌طور منحصر به فرد معین می‌شوند .

(ب) گوییم ایده‌آل P در R ***اولیه*** است اگر $ab \in P$ و $a \notin P$ ایجاب کنند که به‌ازای n ی ، $b^n \in P$. نشان دهیدکه P اولیه‌است اگر و فقط اگر به‌ازای n ی ، $P = (p^n)$ ، که در آن $p \in R$ اول است (= تحویل‌ناپذیراست) یا $p = 0$.

(پ) هرگاه $P_1, P_2, \ldots, P_n$ ایده‌آلهای اولیه‌ای باشند به‌طوری‌که $P_i = (p_i^{n_i})$ و p_i ها عناصر اول متمایزی باشند ، آنگاه $P_1P_2 \cdots P_n = P_1 \cap P_2 \cap \cdots \cap P_n$.

(ت) هر ایده‌آل حقیقی در R را می‌توان (منحصر به فرد صرف‌نظر از ترتیب) به صورت اشتراک تعدادی متناهی ایده‌آل اولیه بیان کرد .

۶ . (آ) هرگاه a و n اعدادی صحیح باشند و $n > 0$ ، آنگاه اعدادی صحیح مانند q و r وجود دارند به‌طوری‌که $a = qn + r$ ، که در آن $|r| \leq n/2$.

(ب) اعداد صحیح گاوسی $\mathbf{Z}[i]$ با $\varphi(a + bi) = a^2 + b^2$ یک دامنهٔ اقلیدسی تشکیل می‌دهند . [**راهنمایی.** برای آنکه نشان دهید که تعریف ۵۰۲ (دو) برقراراست ، ابتدا قرار دهید $y = a + bi$ و فرض کنید x عدد صحیح مثبتی باشد . بنابر قسمت (یک) ، اعداد صحیحی وجود دارند به‌طوری‌که $a = q_1x + r_1$ و $b = q_2x + r_2$ که $|r_1| \leq x/2, |r_2| \leq x/2$. فرض‌کنید $q = q_1 + q_2i$ و $r = r_1 + r_2i$ ؛ در این صورت ، $y = qx + r$ ، که در آن $r = 0$ یا $\varphi(r) < \varphi(x)$. درحالت کلی ، ملاحظه کنید که به‌ازای $x = c + di \neq 0$ و $\bar{x} = c - di$ ، $x\bar{x} > 0$. $q, r_0 \in \mathbf{Z}[i]$ ی وجود دارند به‌طوری‌که $y\bar{x} = q(x\bar{x}) + r_0$ ، که در آن $r_0 = 0$ یا $\varphi(r_0) < \varphi(x\bar{x})$. فرض کنید $r = y - qx$ ؛ در این صورت ، $y = qx + r$ و $r = 0$ یا $\varphi(r) < \varphi(x)$.]

۷ . یکه‌های حلقهٔ اعداد صحیح گاوسی $\mathbf{Z}[i]$ چیستند ؟

۸ . فرض کنید R زیر حلقهٔ زیر از اعداد مختلط باشد :

$$R = \{a + b(1 + \sqrt{19}\, i)/2 \mid a,b \in \mathbf{Z}\}$$

در این صورت ، R یک دامنهٔ ایده‌آل اصلی است که دامنهٔ اقلیدسی نیست .

۹ . فرض کنید R دامنهٔ یکتایی تجزیه بوده و d عنصر ناصفری از R باشد . تنها تعدادی متناهی ایده‌آل اصلی متمایز وجود دارند که شامل ایده‌آل (d) می‌باشند . [**راهنمایی .** $(d) \subset (k) \Rightarrow k \mid d$.]

۱۰ . هرگاه R دامنهٔ یکتایی تجزیه بوده و $a,b \in R$ نسبت به هم اول باشند و $a \mid bc$ ، آنگاه $a \mid c$.

۱۱ . فرض کنید R حلقهٔ اقلیدسی بوده و $a \in R$. در این صورت ، a در R یکه است اگر و فقط اگر $\varphi(a) = \varphi(1_R)$.

۱۲ . هر مجموعهٔ ناتهی از عناصر (احتمالا" نامتناهی) در یک حلقهٔ ایده‌آل اصلی تعویضپذیر یکدار دارای بزرگترین مقسوم‌علیه مشترک است .

۱۳ . (الگوریتم اقلیدسی) . فرض کنید R دامنهٔ اقلیدسی با تابع مربوطهٔ $\varphi : R - \{0\} \to \mathbf{N}$ باشد . اگر $a,b \in R$ و $b \neq 0$ ، روشی برای یافتن بزرگترین مقسوم‌علیه مشترک a و b وجود دارد : با استفادهٔ مکرر از تعریف ۸۰۲ (دو) ، داریم

$$a = q_0 b + r_1 \quad ، \text{که در آن } r_1 = 0 \text{ یا } \varphi(r_1) < \varphi(b) \text{ ؛}$$
$$b = q_1 r_1 + r_2 \quad ، \text{که در آن } r_2 = 0 \text{ یا } \varphi(r_2) < \varphi(r_1) \text{ ؛}$$
$$r_1 = q_2 r_2 + r_3 \quad ، \text{که در آن } r_3 = 0 \text{ یا } \varphi(r_3) < \varphi(r_2) \text{ ؛}$$
$$\vdots$$
$$r_k = q_{k+1} r_{k+1} + r_{k+2} \quad ، \text{که در آن } r_{k+2} = 0 \text{ یا } \varphi(r_{k+2}) < \varphi(r_{k+1}) \text{ ؛}$$
$$\vdots$$

فرض کنید $r_0 = b$ و n کوچکترین عدد صحیحی باشد که $r_{n+1} = 0$ (این n وجود دارد ، زیـرا $\varphi(r_k)$ ها دنباله‌ای اکیدا" نزولی از اعداد صحیح نامنفی را تشکیل می‌دهند) . نشان دهید که r_n بزرگترین مقسوم‌علیه مشترک a و b است .

۴ حلقه‌های خارج‌قسمتها و موضعی سازی

در قسمت اول این بخش، ساخت آشنای میدان اعداد گویا به وسیلهٔ حلقهٔ اعداد صحیح به طـور قابل‌ملاحظه‌ای تعمیم یافت . حلقه‌های خارج‌قسمتها که به این نحو از یک حلقهٔ تعویضپذیر ساخته می‌شوند با خاصیت نگاشت عمومی توصیف می‌شوند (قضیهٔ ۵۰۴) . در آخرین قسمـت این بخش، کـه فقط گهگاه بدان ارجاع خواهد شد ، به ساختار ایده‌آلی (اول) حلقه‌های خارج‌قسمتها پرداخته و موضعی سازی را در یک ایده‌آل اول معرفی می‌کنیم .

تعریف ۱۰۴ . زیرمجموعهٔ ناتهی S از حلقهٔ R **ضربی** است مشروط بر اینکه

$$a,b \in S \Rightarrow ab \in S.$$

چند مثال . مجموعهٔ S مرکب از تمام عناصری‌که در یک حلقهٔ ناصفر یکدار مقسوم‌علیه صفر نبـاشند ، ضربی است . بخصوص، مجموعهٔ تمام عناصر ناصفر از یک دامنهٔ صحیح ضربی است . مجموعهٔ یکه‌ها در یک حلقهٔ یکدار یک مجموعهٔ ضربی است . هرگاه P یک ایده‌آل اول در حلقهٔ تعویضپذیر R باشد ، آنـگاه ، طبق قضیهٔ ۱۵۰۲ ، هر دوی P و $S = R - P$ ضربی‌اند .

انگیزهٔ مطالب زیر را می‌توان در حلقهٔ اعداد صحیح $\mathbf{Z}$ و میدان اعداد گویای $\mathbf{Q}$

به ساده‌ترین وجه دید. واضح است که مجموعهٔ S مرکب از تمام اعداد صحیح ناصفر یک زیرمجموعهٔ ضربی از $\mathbf{Z}$ است. شهودا"، میدان $\mathbf{Q}$ مجموعهٔ تمام کسرهای a/b که $a \in \mathbf{Z}$ و $b \in S$، تحت شرط زیر گرفته می‌شود:

$$a/b = c/d \iff ad = bc \quad (\text{یا } ad - bc = 0)$$

به‌طور دقیقتر، $\mathbf{Q}$ را می‌توان به طریق زیر ساخت (جزئیات برهان بعدا" خواهند آمد). به آسانی معلوم می‌شود که رابطهٔ

$$(a,b) \sim (c,d) \iff ad - bc = 0$$

برمجموعهٔ $\mathbf{Z} \times S$ یک رابطهٔ هم‌ارزی است. $\mathbf{Q}$ مجموعهٔ رده‌های هم‌ارزی $\mathbf{Z} \times S$ تحت این رابطهٔ هم‌ارزی تعریف می‌شود. ردهٔ هم‌ارزی (a,b) با a/b نموده می‌شود و جمع و ضرب به صورت معمول تعریف می‌شوند. می‌توان تحقیق کرد که این اعمال تعریف شده‌اند و $\mathbf{Q}$ تحت آنها میدان می‌باشد. به آسانی معلوم می‌شود که نگاشت $\mathbf{Z} \to \mathbf{Q}$ داده شده با $a \mapsto a/1$ یک تکریختی (نشاننده) است.

حال ساخت ذکرشده در بالا را به یک زیرمجموعهٔ ضربی دلخواه حلقهٔ تعویضپذیر R (احتمالا" بدون واحد) تعمیم می‌دهیم. حلقهٔ تعویضپذیر یکدار $S^{-1}R$ و همریختی $\varphi_S : R \to S^{-1}R$ را می‌سازیم. هرگاه S مجموعهٔ تمام عناصر ناصفر در دامنهٔ صحیح R باشد، آنگاه $S^{-1}R$ یک میدان بوده ($S^{-1}R = \mathbf{Q}$ اگر $R = \mathbf{Z}$) و φ_S یک نشاننده‌ٔ تکریختی R در $S^{-1}R$ است.

قضیهٔ ۲.۴. *فرض کنیم S زیرمجموعه‌ای ضربی از حلقهٔ تعویضپذیر R باشد. رابطهٔ تعریف شده بر مجموعهٔ $R \times S$ به وسیلهٔ*

$$(r,s) \sim (r',s') \iff s_1(rs' - r's) = 0 \text{ ی } s_1 \in S$$

به‌ازای یک رابطهٔ هم‌ارزی است. به علاوه، هرگاه R مقسوم‌علیه صفر نداشته و $0 \notin S$، آنگاه

$$(r,s) \sim (r's') \iff rs' - r's = 0.$$

برهان. تمرین.

فرض کنیم S زیرمجموعه‌ای ضربی از حلقهٔ تعویضپذیر R بوده و $\sim$ رابطهٔ هم‌ارزی قضیهٔ ۲.۴ باشد. ردهٔ هم‌ارزی $(r,s) \in R \times S$ را با r/s نشان می‌دهیم. مجموعهٔ تمام

رده‌های هم‌ارزی $R \times S$ تحت $\sim$ با $S^{-1}R$ نموده می‌شود. تحقیق کنید که

(یک) به‌ازای $s_1 \in S$ ی $s_1(rs' - r's) = 0 \Leftrightarrow r/s = r'/s'$؛

(دو) به‌ازای هر $r \in R$ و $s,t \in S$ ، $tr/ts = r/s$؛

(سه) هرگاه $0 \in S$ ، آنگاه $S^{-1}R$ فقط از یک رده‌ٔ هم‌ارزی تشکیل شده است.

قضیهٔ ۳.۴. *فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر R بوده و $S^{-1}R$ مجموعهٔ رده‌های هم‌ارزی $R \times S$ تحت رابطهٔ هم‌ارزی قضیهٔ ۲.۴ باشد.*

(یک) $S^{-1}R$ حلقه‌ای تعویضپذیر و یکدار است، که در آن جمع و ضرب با

$$r/s + r'/s' = (rs' + r's)/ss' \quad \text{و} \quad (r/s)(r'/s') = rr'/ss'$$

تعریف شده‌اند.

(دو) هرگاه R حلقه‌ای ناصفر بدون مقسوم‌علیه صفر بوده و $0 \notin S$ ، آنگاه $S^{-1}R$ یک دامنهٔ صحیح است.

(سه) هرگاه R حلقه‌ای ناصفر بدون مقسوم‌علیه صفر بوده و S مجموعهٔ تمام عناصر ناصفر R باشد، آنگاه $S^{-1}R$ یک میدان است.

طرح برهان. (یک) به محض آنکه بدانیم جمع و ضرب در $S^{-1}R$ اعمال دوتایی تعریف شده‌ای هستند (مستقل از انتخاب r,s,r',s')، بقیهٔ برهان (یک) به صورت عادی خواهد بود. بخصوص، به‌ازای هر $s,s' \in S$ ، $0/s = 0/s'$ و $0/s$ همانی جمع است. معکوس جمعی r/s عبارت است از $-r/s$. به‌ازای هر $s,s' \in S$ ، $s/s = s'/s'$ و s/s همانی ضربی در $S^{-1}R$ است.

برای نشان دادن اینکه جمع تعریف شده است، ابتدا ملاحظه می‌کنیم که چون S ضربی است، $(rs' + r's)/ss'$ عنصری از $S^{-1}R$ است. اگر $r/s = r_1/s_1$ و $r'/s' = r_1'/s_1'$ ، باید نشان دهیم که

$$(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s_1'$$

طبق فرض، $s_2,s_3 \in S$ ی وجود دارند به‌طوری که

$$s_2(rs_1 - r_1s) = 0,$$
$$s_3(r's_1' - r_1's') = 0.$$

معادلهٔ اول را در $s_3s's_1'$ و معادلهٔ دوم را در s_2ss_1 ضرب می‌کنیم. با جمع معادلات

حاصل، به دست می‌آوریم

$$s_2s_3[(rs' + r's)s_1s_1' - (r_1s_1' + r_1's_1)ss'] = 0.$$

بنابراین، $s_2s_3 \in S$ (زیرا $(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s_1'$) . اثبات مستقل بودن ضرب از r,s,r',s' به همین نحو است.

(دو) هرگاه R مقسوم‌علیه‌صفر نداشته و $0 \notin S$ ، آنگاه $r/s = 0/s$ اگر و فقط اگر در R ، $r = 0$. درنتیجه، در $S^{-1}R$ ، $(r/s)(r'/s') = 0$ اگر و فقط اگر در R ، $rr' = 0$. چون $rr' = 0$ اگر و فقط اگر $r = 0$ یا $r' = 0$ ، نتیجه می‌شود که $S^{-1}R$ یک دامنهٔ صحیح است. (سه) هرگاه $r \neq 0$ ، آنگاه معکوس ضربی $r/s \in S^{-1}R$ مساوی $s/r \in S^{-1}R$ است.

حلقهٔ $S^{-1}R$ در قضیهٔ ۳۰۴ را **حلقهٔ خارج‌قسمتها** یا **حلقهٔ کسرها** یا **حلقهٔ خارج قسمتی** R بر S می‌نامند. یک حالت خاص مهم وقتی رخ می‌دهد که S مجموعهٔ تمام عناصر ناصفر در دامنهٔ صحیح R باشد. در این صورت، $S^{-1}R$ یک میدان است (قضیهٔ ۳۰۴ (سه))که **میدان خارج قسمتی دامنهٔ صحیح** R نام دارد. لذا، اگر $R = \mathbf{Z}$ ، میدان خارج قسمتی درست میدان اعداد گویای $\mathbf{Q}$ است. به‌طورکلی، فرض کنیم R یک حلقهٔ تعویضپذیر ناصفر بوده و S مجموعهٔ تمام عناصر ناصفر R باشد که مقسوم‌علیه صفر نیستند. هرگاه S ناتهی باشد (که در صورت یکدار بودن R همواره چنین است)، آنگاه $S^{-1}R$ حلقهٔ خارج‌قسمتها (یا کسرها)ی تام (یا کامل) حلقهٔ R نامیده می‌شود.[1] قضیهٔ ۳۰۴ (سه) را می‌توان به این صورت بیان کرد: هرگاه R یک حلقهٔ ناصفر بدون مقسوم‌علیه صفر باشد، آنگاه حلقهٔ خارج‌قسمتهای تام R یک میدان است. واضح است که حلقهٔ خارج قسمتهای تام یک دامنهٔ صحیح چیزی جز میدان خارج قسمتی آن نیست.

هرگاه $\varphi : \mathbf{Z} \to \mathbf{Q}$ نگاشت داده‌شده با $n \mapsto n/1$ باشد، آنگاه φ بوضوح یک تکریختی است که $\mathbf{Z}$ را در $\mathbf{Q}$ می‌نشاند. به‌علاوه، به‌ازای هر n ناصفر، $\varphi(n)$ یک یکه در $\mathbf{Q}$ است. به‌طورکلی، داریم

قضیهٔ ۴۰۴. *فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر R باشد.*
(یک) نگاشت $\varphi_S : R \to S^{-1}R$ داده شده با $r \mapsto rs/s$ (به‌ازای هر $s \in S$) یک‌همریختی تعریف شده‌ازحلقه‌هاست به‌طوری‌که $\varphi_S(s)$ ، به‌ازای هر $s \in S$ ، یک یکه در $S^{-1}R$ است.

---

۱. برای مشابه غیرتعویضپذیر، ر.ک. تعریف IX ۷.۴۰ .

(دو) هرگاه $0 \notin S$ و S شامل هیچ مقسوم‌علیه صفر نباشد، آنگاه φ_S یک تکریختی است. بخصوص، هر دامنهٔ صحیح را می‌توان در میدان خارج‌قسمتی خود نشانید.
(سه) هرگاه R یکدار بوده و S از یکه‌ها تشکیل‌شده باشد، آنگاه φ_S یک یکریختی است. بخصوص، حلقهٔ خارج‌قسمتهای تام (= میدان خارج‌قسمتی) میدان F با Γ یکریخت است.

طرح برهان. (یک) هرگاه $s,s' \in S$، آنگاه $rs/s = rs'/s'$، که از آنجا φ_S تعریف شده است. تحقیق کنید که φ_S یک همریختی حلقه‌هاست و به‌ازای هر $s \in S$، $s/s^2 \in S^{-1}R$، معکوس ضربی $\varphi_S(s) = s^2/s$ است. (دو) هرگاه در $S^{-1}R$، $\varphi_S(r) = rs/s = 0$، آنگاه $rs/s = 0/s$، که از آنجا به‌ازای $s_1 \in S$ ی، $rs^2s_1 = 0$. چون $s^2s_1 \in S$، $s^2s_1 \neq 0$. چون S مقسوم‌علیه صفر ندارد، باید داشته باشیم $r = 0$. (سه) بنابر قسمت (دو)، φ_S یک تکریختی است. هرگاه $r/s \in S^{-1}R$ که‌درآن s در R یکه‌است، آنگاه $r/s = \varphi_S(rs^{-1})$، که از آنجا φ_S یک برووریختی است.

در پرتو قضیهٔ ۴.۴ (دو)، رسم است که دامنهٔ صحیح R را با نقش‌آن تحت φ_S یکی کرده و R را زیرحلقهٔ میدان خارج‌قسمتی آن می‌گیرند. چون در این حالت $1_R \in S$، $r \in R$ با $r/1_R \in S^{-1}R$ یکی گرفته می‌شود.

قضیهٔ زیر نشان می‌دهد که حلقه‌های خارج قسمتها را می‌توان کاملا" با خاصیت نگاشت عمومی مشخص کرد. این قضیه گاهی به عنوان تعریف حلقهٔ خارج‌قسمتها گرفته می‌شود.

قضیهٔ ۵.۴. فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر R بوده و T یک حلقهٔ تعویضپذیر یکدار باشد. هرگاه $f: R \to T$ یک همریختی حلقه‌ها باشد به‌طوری‌که $f(s)$، به‌ازای هر $s \in S$، یک یکه در T باشد، آنگاه یک همریختی منحصر به فرد از حلقه‌ها مانند $\bar{f}: S^{-1}R \to T$ وجود دارد به‌طوری که $\bar{f}\varphi_S = f$. حلقهٔ $S^{-1}R$ کاملا" (یا تقریب یکریختی) با این خاصیت معین می‌شود.

طرح برهان. تحقیق کنید که نگاشت $\bar{f}: S^{-1}R \to T$ داده شده با $\bar{f}(r/s) = f(r)f(s)^{-1}$ یک همریختی تعریف شده از حلقه‌هاست به‌طوری که $\bar{f}\varphi_S = f$. هرگاه $g: S^{-1}R \to T$ همریختی دیگری باشد به‌طوری که $g\varphi_S = f$، آنگاه، به‌ازای هر $s \in S$، $g(\varphi_S(s))$ یک

یکه در T است. درنتیجه، بنابرتمرین ۱۵۰۱، به‌ازای‌هر $s \in S$ ، $g(\varphi_S(s)^{-1}) = g(\varphi_S(s))^{-1}$ ، اما، به‌ازای هر $s \in S$، داریم $\varphi_S(s) = s^2/s$ ، که از آنجا $\varphi_S(s)^{-1} = s/s^2 \in S^{-1}R$. لذا، به‌ازای هر $r/s \in S^{-1}R$ ،

$$g(r/s) = g(\varphi_S(r)\varphi_S(s)^{-1}) = g(\varphi_S(r))g(\varphi_S(s)^{-1}) = g(\varphi_S(r))g(\varphi_S(s))^{-1}$$
$$= f(r)f(s)^{-1} = \bar{f}(r/s).$$

بنابراین، $\bar{f} = g$.

برای اثبات آخرین حکم قضیه، فرض‌کنیم $\mathfrak{C}$ رسته‌ای باشد که اشیاء آن تمام (f,T) هایی‌است، که در آنها T یک حلقهٔ تعویضپذیر یکدار بوده و $f : R \to T$ همریختی حلقه‌هاست به‌طوری‌که $f(s)$ ، به‌ازای هر $s \in S$ ، یک یکه در T است. یک ریخت در $\mathfrak{C}$ از (f_1,T_1) به (f_2,T_2) را همریختی $g : T_1 \to T_2$ از حلقه‌ها تعریف می‌کنیم که $gf_1 = f_2$. تحقیق کنید که $\mathfrak{C}$ یک رسته است و ریخت g در $\mathfrak{C}(f_1,T_1) \to (f_2,T_2)$ یک تعادل است اگر و فقط اگر $g : T_1 \to T_2$ یک‌همریختی حلقه‌ها باشد. بند پیش نشان می‌دهد که $(\varphi_S, S^{-1}R)$ یک شیء عمومی در رستهٔ $\mathfrak{C}$ است، که از آنجا، طبق قضیهٔ ۱۰۷۰۱، $S^{-1}R$ کاملا" با یکریختی معین خواهد شد.

نتیجهٔ ۶۰۴ . *فرض‌کنیم R یک‌دامنهٔ صحیح باشد که زیرحلقهٔ میدان خارج‌قسمتی F خود درنظر گرفته شده است. هرگاه E میدان بوده و $f : R \to E$ یک تکریختی حلقه‌ها باشد، آنگاه تکریختی منحصر به فردی از میدانها مانند $\bar{f} : F \to E$ وجود دارد به‌طوری‌که $\bar{f} \mid R = f$. بخصوص، هر میدان E_1 شامل R شامل یک نسخهٔ یکریخت F_1 از F است که $R \subset F_1 \subset E_1$.*

طرح برهان. فرض‌کنیم S مجموعهٔ تمام عناصر ناصفر R بوده و قضیهٔ ۵۰۴ را درمورد $f : R \to E$ اعمال می‌کنیم. در این صورت، یک‌همریختی مانند $\bar{f} : S^{-1}R = F \to E$ وجود دارد به‌طوری که $\bar{f}\varphi_S = f$. تحقیق کنید که $\bar{f}$ یک تکریختی است. چون R با $\varphi_S(R)$ یکی گرفته شده، پس $\bar{f} \mid R = f$. آخرین حکم قضیه حالت خاصی است که در آن $f : R \to E_1$ نگاشت شمول است.

قضایای ۷۰۴ تا ۱۱۰۴ به ساختار ایده‌آلی حلقه‌های خارج‌قسمتها می‌پردازند: این

مطالب فقط در بخش VIII ۶۰ به کار می‌روند. قضیهٔ ۱۳.۴، که به قضایای ۷.۴ تا ۱۱.۴ وابسته نیست، در آینده مورد ارجاع واقع خواهد شد.

قضیهٔ ۷.۴. فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر R باشد.
(یک) هرگاه I یک ایده‌آل در R باشد، آنگاه $S^{-1}I = \{a/s | a \in I; s \in S\}$ یک ایده‌آل در $S^{-1}R$ است.
(دو) هرگاه J ایده‌آل دیگری در R باشد، آنگاه

$$S^{-1}(I + J) = S^{-1}I + S^{-1}J;$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J);$$
$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J.$$

چند تبصره. $S^{-1}I$ را توسیع I در $S^{-1}R$ می‌نامند. توجه کنید که $r/s \in S^{-1}I$ لزوماً $r \in I$ را ایجاب نمی‌کند، زیرا ممکن است داشته باشیم $a/s = r/s$ که در آن $a \in I, r \notin I$.

طرح برهان ۷.۴. از این امر استفاده کنید که در $S^{-1}R$، $\sum_{i=1}^{n} (c_i/s) = \left(\sum_{i=1}^{n} c_i\right)/s$؛

$$\text{و} \quad \sum_{j=1}^{m} (a_i b_j/s) = \sum_{j=1}^{m} (a_i/s)(b_j s/s)$$

$$\sum_{k=1}^{t} (c_k/s_k) = \left(\sum_{k=1}^{t} c_k s_1 s_2 \cdots s_{k-1} s_{k+1} \cdots s_t\right)/s_1 s_2 \cdots s_t.$$

قضیهٔ ۸.۴. فرض کنید S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر و یکدار R بوده و I ایده‌آلی از R باشد. در این صورت، $S^{-1}I = S^{-1}R$ اگر و فقط اگر $S \cap I \neq \varnothing$.

برهان. هرگاه $s \in S \cap I$، آنگاه $1_{S^{-1}R} = s/s \in S^{-1}I$، و درنتیجه، $S^{-1}I = S^{-1}R$. به‌عکس، هرگاه $S^{-1}I = S^{-1}R$، آنگاه $\varphi_S^{-1}(S^{-1}I) = R$، که از آنجا، به‌ازای $a \in I, s \in S$ ای، $\varphi_S(1_R) = a/s$. چون $\varphi_S(1_R) = 1_R s/s$، به‌ازای $s_1 \in S$ ی داریم $s^2 s_1 = a s s_1$. اما $s^2 s_1 \in S$ و $a s s_1 \in I$ ایجاب می‌کند که $I \cup S \neq \varnothing$.

برای مشخص کردن ایده‌آلهای اول در یک حلقهٔ خارج‌قسمتها، به یک لم نیاز داریم. به یاد آورید که هرگاه J ایده‌آلی در حلقهٔ خارج قسمتهای $S^{-1}R$ باشد، آنگاه $\varphi_S^{-1}(J)$ ایده‌آلی در R است (تمرین ۱۳۰۲). $\varphi_S^{-1}(J)$ را گاهی *انقباض* J در R می‌نامند.

لم ۹۰۴. *فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر یکدار R بوده و I ایده‌آلی در R باشد.*

(یک) $I \subset \varphi_S^{-1}(S^{-1}I)$.

(دو) *هرگاه به‌ازای ایده‌آلی چون J در $S^{-1}R$، $I = \varphi_S^{-1}(J)$، آنگاه $S^{-1}I = J$. به عبارت دیگر، هر ایده‌آل در $S^{-1}R$ به‌ازای ایده‌آلی چون I در R به شکل $S^{-1}I$ است.*

(سه) *هرگاه P ایده‌آل اولی در R بوده و $S \cap P = \varnothing$، آنگاه $S^{-1}P$ ایده‌آل اولی در $S^{-1}R$ است و $\varphi_S^{-1}(S^{-1}P) = P$.*

برهان. (یک) هرگاه $a \in I$، آنگاه به‌ازای هر $s \in S$، $as \in I$. در نتیجه، $\varphi_S(a) = as/s \in S^{-1}I$، که از آنجا $a \in \varphi_S^{-1}(S^{-1}I)$. بنابراین، $I \subset \varphi_S^{-1}(S^{-1}I)$.

(دو) چون $I = \varphi_S^{-1}(J)$، هر عنصر $S^{-1}I$ به شکل r/s است، که در آن $\varphi_S(r) \in J$. بنابراین، $r/s = (1_R/s)(rs/s) = (1_R/s)\varphi_S(r) \in J$، که‌ازآنجا $S^{-1}I \subset J$. به عکس، هرگاه $r/s \in J$، آنگاه $\varphi_S(r) = rs/s = (r/s)(s^2/s) \in J$، که از آنجا $r \in \varphi_S^{-1}(J) = I$. لذا، $r/s \in S^{-1}I$؛ و درنتیجه، $J \subset S^{-1}I$. (سه) بنابر قضیهٔ ۸۰۴، $S^{-1}P$ ایده‌آلی است که $S^{-1}P \neq S^{-1}R$. هرگاه $(r/s)(r'/s') \in S^{-1}P$، آنگاه $rr'/ss' = a/t$ که در آن $a \in P, t \in S$. درنتیجه، به‌ازای $s_1 \in S$ ی، $s_1trr' = s_1ss'a \in P$. چون $s_1t \in S$ و $S \cap P = \varnothing$، قضیهٔ ۱۵۰۲ ایجاب می‌کند که $rr' \in P$، که از آنجا $r \in P$ یا $r' \in P$. لذا، $r/s \in S^{-1}P$ یا $r'/s' \in S^{-1}P$. بنابراین، طبق قضیهٔ ۱۵۰۲، $S^{-1}P$ اول است. بالاخره، طبق (یک)، $P \subset \varphi_S^{-1}(S^{-1}P)$. به عکس، هرگاه $r \in \varphi_S^{-1}(S^{-1}P)$، آنگاه $\varphi_S(r) \in S^{-1}P$. لذا، $\varphi_S(r) = rs/s = a/t$ که در آن $a \in P$ و $s, t \in S$. درنتیجه، به‌ازای $s_1 \in S$ ی، $s_1str = s_1sa \in P$. چون $s_1st \in S$ و $S \cap P = \varnothing$، طبق قضیهٔ ۱۵۰۲، $r \in P$. بنابراین، $\varphi_S^{-1}(S^{-1}P) \subset P$.

قضیهٔ ۱۰۰۴. *فرض کنیم S یک زیرمجموعهٔ ضربی حلقهٔ تعویضپذیر یکدار R باشد. در این صورت، تناظر یک به یکی بین مجموعهٔ $\mathfrak{U}$ از ایده‌آلهای اول R که جدا از S اند*

و مجموعهٔ $\mathfrak{U}$ از ایده‌آلهای اول $S^{-1}R$ وجود دارد که با $P \mapsto S^{-1}P$ داده می‌شود.

برهان. بنابر لم ۹۰۴ (سه)، ارتباط $P \mapsto S^{-1}P$ یک نگاشت انژکتیو $\mathfrak{U} \to \mathfrak{u}$ تعریف می‌کند. کافی است نشان دهیم که این نگاشت سورژکتیو نیز هست. فرض کنیم J یک ایده‌آل اول $S^{-1}R$ باشد و قرار می‌دهیم $P = \varphi_S^{-1}(J)$. چون طبق لم ۹۰۴ (دو) $S^{-1}P = J$، کافی است نشان دهیم که P اول است. هرگاه $ab \in P$، آنگاه $\varphi_S(a)\varphi_S(b) = \varphi_S(ab) \in J$، زیرا $P = \varphi_S^{-1}(J)$. چون J در $S^{-1}R$ اول است، طبق قضیهٔ ۱۵۰۲، $\varphi_S(a) \in J$ یا $\varphi_S(b) \in J$. درنتیجه، $a \in \varphi_S^{-1}(J) = P$ یا $b \in P$. بنابراین، طبق قضیهٔ ۱۵۰۲، P اول است.

فرض کنیم R یک حلقهٔ تعویضپذیر یکدار بوده و P ایده‌آل اولی از R باشد. در این صورت، طبق قضیهٔ ۱۵۰۲، $S = R - P$ یک زیرمجموعهٔ ضربی از R است. حلقهٔ خارج قسمتهای $S^{-1}R$ **موضعی سازی R در P** نام دارد و با نماد R_P نموده می‌شود. هرگاه I ایده‌آلی در R باشد، آنگاه ایده‌آل $S^{-1}I$ در R_P با I_P نموده می‌شود.

قضیهٔ ۱۱۰۴. فرض کنیم P یک ایده‌آل اول در حلقهٔ تعویضپذیر یکدار R باشد.
(یک) تناظر یک به یکی بین مجموعهٔ ایده‌آلهای اول R که مشمول P اند و مجموعهٔ ایده‌آلهای اول R_P وجود دارد که با $Q \mapsto Q_P$ داده می‌شود.
(دو) ایده‌آل P_P در R_P ایده‌آل ماکزیمال منحصر به فرد R_P می‌باشد.

برهان. چون ایده‌آلهای اول R مشمول P درست آنهایی هستند که از $S = R - P$ جدایند، (یک) نتیجهٔ فوری قضیهٔ ۱۰۴۰۴ می‌باشد. هرگاه M ایده‌آل ماکزیمال R_P باشد، آنگاه طبق قضیهٔ ۱۹۰۲، M اول است، که از آنجا، به‌ازای ایده‌آل اولی چون Q از R که $Q \subset P$، $M = Q_P$. اما $Q \subset P$ ایجاب می‌کند که $Q_P \subset P_P$. چون طبق قضیهٔ ۸۰۴ $P_P \neq R_P$، باید داشته باشیم $Q_P = P_P$. بنابراین، P_P ایده‌آل ماکزیمال منحصر به فردی در R_P می‌باشد.

حلقه‌های دارای ایده‌آل ماکزیمال منحصر به فرد، نظیر R_P در قضیهٔ ۱۱۰۴، به

خودی خود جالب توجه‌اند .

تعریف ۱۲۰۴ . یک **حلقهٔ موضعی** حلقهٔ تعویضپذیر یکداری است که ایده‌آل ماکزیمال منحصر به فرد دارد .

تبصره . چون هر ایده‌آل در یک حلقهٔ یکدار مشمول ایده‌آل ماکزیمالی است (قضیهٔ ۱۸۰۲) ، ایده‌آل ماکزیمال منحصر به فرد حلقهٔ موضعی R باید هر ایده‌آل R (البته غیر از خود R) را شامل باشد .

مثال . هرگاه p اول بوده و $n \geq 1$ ، آنگاه Z_{p^n} یک حلقهٔ موضعی با ایده‌آل ماکزیمال منحصر به فرد (p) است .

قضیهٔ ۱۳۰۴ . ***هرگاه R یک حلقهٔ تعویضپذیر یکدار باشد ، آنگاه شرایط زیر معادلند :***

(یک) R یک حلقهٔ موضعی است ؛

(دو) تمام غیر یکه‌های R مشمول ایده‌آلی مانند $M \neq R$ اند ؛

(سه) غیر یکه‌های R یک ایده‌آل تشکیل می‌دهند .

طرح برهان . هرگاه I ایده‌آلی از R بوده و $a \in I$ ، آنگاه ، بنابر قضیهٔ ۵۰۲ ، $(a) \subset I$. درنتیجه ، $I \neq R$ اگر و فقط اگر I فقط از غیریکه‌ها تشکیل شده باشد (قضیهٔ ۲۰۳ (چهار)) . (سه) $\Rightarrow$ (دو) و (یک) $\Rightarrow$ (سه) از امر نتیجه می‌شوند . (دو) $\Rightarrow$ (یک) . هرگاه $a \in R$ یک غیریکه باشد ، آنگاه $(a) \neq R$. بنابراین ، طبق تبصرهٔ بعد از تعریف ۱۲۰۴ ، (a) (و درنتیجه ، a) مشمول ایده‌آل ماکزیمال منحصر به فرد R است .

تمرینات

۱ . حلقهٔ خارج قسمتهای حلقهٔ Z_n را به‌ازای هر $n \geq 2$ تعیین کنید .

۲ . فرض کنید S زیرمجموعه‌ای ضربی از حلقهٔ تعویضپذیر یکدار R بوده و T یک زیرمجموعهٔ ضربی حلقهٔ $S^{-1}R$ باشد . فرض کنید

$$S_* = \{r \in R \mid r/s \in T \text{ ، ی } s \in S \text{ به‌ازای }\}$$

در این صورت، S_* یک زیرمجموعهٔ ضربی R بوده و یک یکریختی حلقه‌ها مانند $S_*^{-1}R \cong T^{-1}(S^{-1}R)$ وجود دارد.

۳. (آ) مجموعهٔ E مرکب از اعداد صحیح زوج مثبت یک زیرمجموعهٔ ضربی $\mathbf{Z}$ است به‌طوری که $E^{-1}(\mathbf{Z})$ میدان اعداد گویاست.

(ب) شرط(هایی) بر زیرمجموعهٔ ضربی S از $\mathbf{Z}$ بیان و ثابت کنید که تضمین کند که $S^{-1}\mathbf{Z}$ میدان اعداد گویاست.

۴. هرگاه $S = \{2,4\}$ و $R = Z_6$، آنگاه $S^{-1}R$ با میدان Z_3 یکریخت است. درنتیجه، عکس قضیهٔ ۳.۴ (دو) نادرست است.

۵. فرض کنید R یک دامنهٔ صحیح با میدان خارج‌قسمتی F باشد. هرگاه T دامنهٔ صحیحی باشد که $R \subset T \subset F$، آنگاه F میدان خارج‌قسمتی T است (با آن یکریخت است).

۶. فرض کنید S یک زیرمجموعهٔ ضربی دامنهٔ صحیح R باشد به‌طوری‌که $0 \notin S$. هرگاه R یک دامنهٔ ایده‌آل اصلی [یا دامنهٔ یکتایی تجزیه] باشد، آنگاه $S^{-1}R$ نیز چنین است.

۷. فرض کنید R_1 و R_2 دامنه‌های صحیحی به ترتیب با میدانهای F_1 و F_2 باشند. هرگاه $f : R_1 \to R_2$ یک یکریختی باشد، آنگاه f به یک یکریختی مانند $F_1 \cong F_2$ قابل توسیع است. [**راهنمایی.** نتیجهٔ ۶.۴]

۸. فرض کنید R یک حلقهٔ تعویضپذیر یکدار بوده، I یک ایده‌آل R باشد، و $\pi : R \to R/I$ تصویر کانونی باشد.

(آ) هرگاه S یک زیرمجموعهٔ ضربی R باشد، آنگاه $\pi S = \pi(S)$ یک زیرمجموعهٔ ضربی R/I است.

(ب) نگاشت $\theta : S^{-1}R \to (\pi S)^{-1}(R/I)$ داده‌شده با $r/s \mapsto \pi(r)/\pi(s)$ یک تابع تعریف شده است.

(پ) θ یک برووریختی حلقه‌ها با هستهٔ $S^{-1}I$ است؛ و درنتیجه، یک یکریختی حلقه‌ها مانند $S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I)$ را القا می‌کند.

۹. فرض کنید S یک زیرمجموعهٔ ضربی از حلقهٔ تعویضپذیر یکدار R باشد. هرگاه I یک ایده‌آل در R باشد، آنگاه $S^{-1}(\mathrm{Rad}\ I) = \mathrm{Rad}\ (S^{-1}I)$. [ر.ک. تمرین ۲.۲۰]

۱۰. فرض کنید R دامنهٔ صحیح بوده و به‌ازای هر ایده‌آل ماکزیمال M (که، البته، اول

نیزهست) ، R_M را به عنوان یک زیرحلقه از میدان خارج‌قسمتی R درنظر بگیرید . نشان دهید که $R = \cap R_M$ ، که در آن اشتراک روی تمام ایده‌آلهای ماکزیمال M از R گرفته شده است .

۱۱ . فرض کنید p یک عدد اول در $\mathbf{Z}$ باشد ؛ دراین صورت ، (p) یک ایده‌آل اول است . در باب رابطهٔ Z_p و موضعی سازی $\mathbf{Z}_{(p)}$ چه می‌شود گفت ؟

۱۲ . یک حلقهٔ تعویضپذیر یکدار موضعی است اگر و فقط اگر به‌ازای هر $r, s \in R$ ، $r + s = 1_R$ ایجاب کند که r یا s یکه است .

۱۳ . حلقهٔ R مرکب از تمام اعداد گویا با مخرجهایی که بر عدد اولی (ثابتی) چون p بخشپذیر نیستند یک حلقهٔ موضعی است .

۱۴ . هرگاه M درحلقهٔ تعویضپذیر یکدار R یک ایده‌آل ماکزیمال بوده و n عدد صحیح مثبتی باشد ، آنگاه حلقهٔ R/M^n ایده‌آل اول منحصر به فرد دارد ؛ و لذا ، موضعی است .

۱۵ . در حلقهٔ تعویضپذیر یکدار R شرایط زیر معادلند :

(یک) R دارای ایده‌آل اول منحصر به فرد است ؛ (دو) هر غیر یکه پوچ توان است (ر.ک. تمرین ۱۲۰۱) ؛

(سه) R دارای ایده‌آل اول مینیمال است که شامل تمام مقسوم علیه‌های صفر است ، و تمام غیریکه‌های R مقسوم علیه‌های صفر می‌باشند .

۱۶ . هر نقش همریخت ناصفر یک حلقهٔ موضعی ، موضعی است .

۵ حلقه‌های چندجمله‌ایها و سریهای توانی صوری

بحث را با تعریف و ارائهٔ نمادها برای چندجمله‌ایهای یک مجهولی روی حلقهٔ R آغاز می‌کنیم . سپس حلقهٔ چندجمله‌ایهای n مجهولی روی R تعریف شده و خواص اساسی آن عرضه خواهد شد . قسمت آخر بخش ، که بعداً لازم نمی‌شود ، آشنایی مختصری با حلقهٔ سریهای توانی صوری یک مجهولی روی R است .

قضیهٔ ۱۰۵ . *فرض کنیم* R *یک حلقه بوده و* $R[x]$ *مجموعهٔ تمام دنباله‌ها از عناصر* R *باشند* $(a_0, a_1, \ldots)$ *باشد به‌طوری‌که به‌ازای هر* i *جز تعدادی متناهی ،* $a_i = 0$.

(یک) $R[x]$ *حلقه‌ای است با جمع و ضربی که به صورت زیر تعریف می‌شوند :*

$$(a_0,a_1,\ldots)+(b_0,b_1,\ldots)=(a_0+b_0,a_1+b_1,\ldots)$$

و

$$(a_0,a_1,\ldots)(b_0,b_1,\ldots)=(c_0,c_1,\ldots),$$

که در آن

$$c_n=\sum_{i=0}^{n}a_{n-i}b_i=a_nb_0+a_{n-1}b_1+\cdots+a_1b_{n-1}+a_0b_n=\sum_{k+j=n}a_kb_j.$$

(دو) هرگاه R تعویضپذیر [یا حلقه‌ای یکدار یا حلقه‌ای بدون مقسوم‌علیه صفر یا دامنهٔ صحیح] باشد، آنگاه $R[x]$ نیز چنین است.

(سه) نگاشت $R\to R[x]$ داده شده با $r\mapsto(r,0,0,\ldots)$ یک تکریختی از حلقه‌هاست.

برهان. تمرین. هرگاه R دارای واحد 1_R باشد، آنگاه $(1_R,0,0,\ldots)$ یک واحد در $R[x]$ است. ملاحظه کنید هرگاه $(a_0,a_1,\ldots),(b_0,b_1,\ldots)\in R[x]$ و k [یا j] کوچکترین اندیسی باشد که $a_k\neq 0$ [یا $b_j\neq 0$]، آنگاه

$$(a_0,a_1,\ldots)(b_0,b_1,\ldots)=(0,\ldots,0,a_kb_j,a_{k+1}b_j+a_kb_{j+1},\ldots).$$

حلقهٔ $R[x]$ قضیهٔ ۱۰۵ **حلقهٔ چندجمله‌ایها** روی R نام دارد. عنصرهای آن **چندجمله‌ای** نامیده می‌شوند. نماد $R[x]$ در زیر توضیح داده شده است. در پرتو قضیهٔ ۱۰۵ (سه) R را با نقش یکریخت آن در $R[x]$ یکی کرده و به جای $(r,0,0,\ldots)$ فقط r می‌نویسیم. توجه کنید که $r(a_0,a_1,\ldots)=(ra_0,ra_1,\ldots)$. حال نماد آشناتری برای چندجمله‌ایها عرضه می‌کنیم.

قضیهٔ ۲۰۵. فرض کنیم R یک حلقهٔ یکدار بوده و عنصر $(0,1_R,0,0,\ldots)$ از $R[x]$ با x نشان داده شده باشد.

(یک) $x^n=(0,0,\ldots,0,1_R,0,\ldots)$، که در آن 1_R مختص $(n+1)$ ام است.

(دو) هرگاه $r\in R$. آنگاه به‌ازای هر $n\geq 0$، $rx^n=x^nr=(0,\ldots,0,r,0,\ldots)$، که در آن r مختص $(n+1)$ ام است.

(سه) به‌ازای هرچندجمله‌ای ناصفر f در $R[x]$، عدد صحیحی مانند $n\in\mathbf{N}$ و عناصری چون $a_0,\ldots,a_n\in R$ وجود دارند به‌طوری‌که $f=a_0x^0+a_1x^1+\cdots+a_nx^n$. عدد صحیح

n و عنصرهای a_i منحصربه‌فرد ند بدین معنی که $(b_i \in R)\ f = b_0x^0 + b_1x^1 + \cdots + b_mx^m$ ایجاب می‌کند که $m \geq n$ ؛ به‌ازای $i = 1,2,\ldots,n$ ، $a_i = b_i$ ؛ و به‌ازای $n < i \leq m$ ، $b_i = 0$.

طرح برهان. در مورد (یک) استقرا به کار برید و (دو) را مستقیما" حساب کنید. (سه) اگر $f = (a_0,a_1,\ldots) \in R[x]$ ، باید بزرگترین اندیس n که $a_n \neq 0$ وجود داشته باشد. در این صورت ، $a_0,a_1,\ldots,a_n \in R$ عناصر مطلوب می‌باشند.

هرگاه R یکدار باشد ، آنگاه $x^0 = 1_R$ (همانند در هر حلقهٔ یکدار) و چندجمله‌ای $f = a_0x^0 + a_1x^1 + \cdots + a_nx^n$ را به صورت $f = a_0 + a_1x + \cdots + a_nx^n$ می‌نویسیم. شایسته است نمادگذاری قضیهٔ ۲.۵ را به حلقه‌های بدون واحد به صورت زیر تعمیم دهیم. هرگاه R حلقه‌ای بدون واحد باشد ، آنگاه ، بنابر قضیهٔ ۱۰.۱ ، R را می‌توان در حلقهٔ یکداری مانند S نشانید. R را با نقش آن تحت نگاشت نشاننده یکی می‌کنیم ؛ درنتیجه ، R یک زیرحلقهٔ S است. پس $R[x]$ بوضوح یک زیرحلقهٔ $S[x]$ می‌باشد. درنتیجه ، هر چندجمله‌ای $f = (a_0,a_1,\ldots) \in R[x]$ را می‌توان به‌طور منحصر به فرد به صورت $f = a_0 + a_1x^1 + \cdots + a_nx^n$ نوشت ، که در آن $a_i \in R \subset S$ ، $a_n \neq 0$ ، و $x = (0,1_S,0,0,\ldots) \in S[x]$. تنها اختلاف مهم بین این و حالتی که R واحد دارد این است که در این حالت عنصر x در $R[x]$ نیست.

از اینجا به بعد چندجمله‌ای f روی حلقهٔ R (با یا بدون واحد) همواره به شکل $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ $(a_i \in R)$ نوشته می‌شود. با این نماد ، جمع و ضرب در $R[x]$ با قواعد آشنای زیر تعریف می‌شوند :

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i$$

$$\left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{m} b_jx^j\right) = \sum_{k=0}^{m+n} c_kx^k \text{ ، که در آن } c_k = \sum_{i+j=k} a_ib_j \text{ .}$$

هرگاه $f = \sum_{i=0}^{n} a_ix^i \in R[x]$ ، آنگاه عناصر $a_i \in R$ **ضرایب** f نام دارند. عنصر a_0 **جملهٔ ثابت** نامیده می‌شود. عناصر R ، که همه به شکل $r = (r,0,0,\ldots) = rx^0$ می‌باشند ،

چندجمله‌ایهای ثابت نامیده می‌شوند . هرگاه

$$f = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n = a_n x^n + \cdots + a_1 x + a_0$$

دارای $a_n \neq 0$ باشد ،آنگاه a_n **ضریب پیشرو** f نام دارد . هرگاه R یکدار و ضریب پیشرو 1_R باشد ، آنگاه گوییم f یک **چندجمله‌ای تکین** است .

فرض کنیم R یک حلقه (یکدار) باشد . به دلایل تاریخی ، عنصر $x = (0,1_R,0,\ldots)$ از $R[x]$ یک **مجهول** نام دارد . می‌توان از چندجمله‌ایها از مجهول x سخن گفت . هرگاه S حلقهٔ (یکدار) دیگری باشد ، آنگاه مجهول $x \in S[x]$ همان عنصر $x \in R[x]$ **نیست** . این نماد مبهم اشکالی ایجاد نمی‌کند .

اگر R یک حلقه باشد ،گاهی شایسته است یک نسخه از حلقهٔ چندجمله‌ای روی R از دیگری متمایزشود . در این وضع مجهول در یک نسخه با یک علامت ، مثلا " x " ، و در نسخهٔ دیگر با علامتی متفاوت ، مثلا " y " ، نموده می‌شود . در حالت اخیر ، حلقهٔ چندجمله‌ای با $R[y]$ نموده شده و عناصرش به شکل $a_0 + a_1 y + \cdots + a_n y^n$ می‌باشند .

حال چندجمله‌ایهای با بیش از یک مجهول را تعریف می‌کنیم . برای تسهیل در بحث ، به تعدادی متناهی مجهول محدود می‌شویم . برای حالت کلی ، ر.ک. تمرین ۴ . تعریف از این ناشی شده است که یک چندجمله‌ای یک مجهولی حالت خاصی از دنباله، یعنی تابعی چون $\mathbf{N} \to R$ ، تعریف می‌شود . به‌ازای هر عدد صحیح مثبت n ، فرض کنیم $\mathbf{N}^n = \mathbf{N} \times \cdots \times \mathbf{N}$ (n عامل) . عناصر $\mathbf{N}^n$ ، n تاییهای مرتبی از عناصر $\mathbf{N}$ می‌باشند . واضح است که $\mathbf{N}^n$ یک تکگون آبلی جمعی تحت جمع مختص به مختص است .

قضیهٔ ۳.۵ . فرض کنیم R **یک حلقه بوده و** $R[x_1, \ldots, x_n]$ **مجموعهٔ تمام توابع** $f : \mathbf{N}^n \to R$ **باشد به‌طوری‌که به‌ازای حداکثر تعدادی متناهی عنصر** u **از** $\mathbf{N}^n$ **،** $f(u) \neq 0$ **.**
(یک) $R[x_1, \ldots, x_n]$ **یک حلقه با جمع و ضرب تعریف شده با**

$$(f+g)(u) = f(u) + g(u) \quad \text{و} \quad (fg)(u) = \sum_{\substack{v+w=u \\ v,w \in \mathbf{N}^n}} f(v)g(w)$$

است ، که در آنها $f,g \in R[x_1, \ldots, x_n]$ **و** $u \in \mathbf{N}^n$ **.**
(دو) هرگاه R **تعویضپذیر [یا حلقه‌ای یکدار یا حلقه‌ای بدون مقسوم‌علیه صفر یا دامنهٔ صحیح] باشد ، آنگاه** $R[x_1, \ldots, x_n]$ **نیز چنین است .**

(سه) نگاشت $R \to R[x_1, \ldots, x_n]$ داده شده با $r \mapsto f_r$، که در آن $f_r(0, \ldots, 0) = r$ و به‌ازای هر $u \in N^n$ ی دیگر، $f(u) = 0$، یک تکریختی از حلقه‌هاست.

برهان. تمرین.

حلقهٔ $R[x_1, \ldots, x_n]$ قضیهٔ ۳۰۵ حلقهٔ چندجمله‌ایها از n مجهول روی R نام دارد. R با نقش یکریخت خود تحت نگاشت قضیهٔ ۳۰۵ (سه) یکی شده و یک زیرحلقهٔ $R[x_1, \ldots, x_n]$ درنظرگرفته‌می‌شود. هرگاه $n = 1$، آنگاه $R[x_1]$ درست حلقهٔ چندجمله‌ایها مثل قضیهٔ ۱۰۵ است. مثل چندجمله‌ایهای یک مجهولی، نماد مناسبتری برای عناصر $R[x_1, \ldots, x_n]$ وجود دارد.

فرض کنیم n یک عدد صحیح مثبت بوده و به‌ازای هر $i = 1,2, \ldots, n$، قرار می‌دهیم

$$\varepsilon_i = (0, \ldots, 0,1,0, \ldots, 0) \in N^n,$$

که در آن 1 مختص i ام ε_i است. اگر $k \in N$، قرار می‌دهیم $k\varepsilon_i = (0, \ldots, 0,k,0, \ldots 0)$. در این صورت، هر عنصر N^n را می‌توان به شکل $k_1\varepsilon_1 + k_2\varepsilon_2 + \cdots + k_n\varepsilon_n$ نوشت.

قضیهٔ ۴۰۵. فرض کنیم R یک حلقهٔ یکدار بوده و n عدد صحیح مثبتی باشد. به‌ازای هر $i = 1,2, \ldots, n$، $x_i \in R[x_1, \ldots, x_n]$ را با $x_i(\varepsilon_i) = 1_R$ و، به‌ازای $u \neq \varepsilon_i$ با $x_i(u) = 0$ تعریف می‌کنیم.

(یک) به‌ازای هر عدد صحیح $k \in N$، $x_i^k(k\varepsilon_i) = 1_R$، و به‌ازای $u \neq k\varepsilon_i$، $x_i^k(u) = 0$؛

(دو) به‌ازای هر $(k_1, \ldots, k_n) \in N^n$، $x_1^{k_1}x_2^{k_2} \cdots x_n^{k_n}(k_1\varepsilon_1 + \cdots + k_n\varepsilon_n) = 1_R$، و به‌ازای $u \neq k_1\varepsilon_1 + \cdots + k_n\varepsilon_n$، $x_1^{k_1}x_2^{k_2} \cdots x_n^{k_n}(u) = 0$؛

(سه) به‌ازای هر $s,t \in N$ و هر $i,j = 1,2, \ldots, n$، $x_i^s x_j^t = x_j^t x_i^s$؛

(چهار) به‌ازای هر $r \in R$ و هر $t \in N$، $x_i^t r = r x_i^t$؛

(پنج) به‌ازای هر چندجمله‌ای ناصفر f در $R[x_1, \ldots, x_n]$، عناصر ناصفر منحصر به‌فردی مانند $(k_{11},k_{12}, \ldots, k_{1n}),(k_{21},k_{22}, \ldots, k_{2n}), \ldots, (k_{m1},k_{m2}, \ldots, k_{mn})$ از N^n و عنصرهای منحصر به فردی مانند $a_0,a_1, \ldots, a_m$ از R وجود دارند به‌طوری‌که

$$f = a_0x_1^0x_2^0 \cdots x_n^0 + a_1x_1^{k_{11}}x_2^{k_{12}} \cdots x_n^{k_{1n}}$$

$$+ a_2x_1^{k_{21}}x_2^{k_{22}}\cdots x_n^{k_{2n}} + \cdots + a_mx_1^{k_{m1}}x_2^{k_{m2}}\cdots x_n^{k_{mn}}.$$

طرح برهان. (پنج) فرض کنید $(k_{11}, \ldots, k_{1n}), \ldots, (k_{m1}, \ldots, k_{mn})$ آن عناصر ناصفری از $\mathbf{N}^n$ باشند که f بر آنها ناصفر است. فرض کنید $a_0 = f(0, \ldots, 0)$ و، به‌ازای $i = 1,2, \ldots, m$، قرار دهید $a_i = f(k_{i1}, k_{i2}, \ldots, k_{in})$.

هرگاه R حلقه‌ای یکدار باشد، آنگاه، مثل قضیهٔ ۴۰۵، عناصر $x_1, x_2, \ldots, x_n \in R[x_1, \ldots, x_n]$ **مجهولات** نام دارند. مثل حالت یک مجهولی، هرجا مناسب باشد، از علایمی غیر از $x_1, \ldots, x_n$ برای نشان دادن مجهولات استفاده می‌کنیم. عنصرهای $a_0, a_1, \ldots, a_m$ در قضیهٔ ۴۰۵ (پنج) **ضرایب** چندجمله‌ای f نام دارند. یک چندجمله‌ای به شکل $(a \in R)\ ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ یک **تکجمله‌ای** از $x_1, x_2, \ldots, x_n$ نامیده می‌شود. قضیهٔ ۴۰۵ (پنج) نشان می‌دهد که هرچندجمله‌ای مجموعی از تکجمله‌ایهاست. در یک تکجمله‌ای معمولاً آن x_i هایی را که نمای صفر دارند حذف می‌کنند. مثلاً "، $a_0 + a_1x_1^2x_3 + a_2x_1x_2^3x_3$ نوشته می‌شود. نماد $a_0x_1^0x_2^0x_3^0 + a_1x_1^2x_2^0x_3 + a_2x_1x_2^3x_3$ به شکل $R[x_1, \ldots, x_n]$، که در آن R فاقد واحد است، واصطلاح قضیهٔ ۴۰۵ به حلقهٔ چندجمله‌ای درست مثل حالت یک مجهولی، تعمیم یافته‌اند. حلقهٔ R در یک حلقهٔ یکدار S نشانیده شده و $R[x_1, \ldots, x_n]$ زیرحلقهٔ $S[x_1, \ldots, x_n]$ درنظر گرفته شده است. هرگاه R یکدار نباشد، آنگاه مجهولات $x_1, x_2, \ldots, x_n$ و تکجمله‌ایهای $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ $(k_i \in \mathbf{N})$ عناصری از $R[x_1, \ldots, x_n]$ نیستند.

هرگاه R یک حلقه باشد، آنگاه به‌آسانی دیده می‌شود که نگاشت $R[x_1] \to R[x_1, \ldots, x_n]$ تعریف شده با $\sum_{i=0}^{m} a_ix_1^i \mapsto \sum_{i=0}^{m} a_ix_1^ix_2^0\cdots x_n^0 = \sum_{i=0}^{m} a_ix_1^i \in R[x_1, \ldots, x_n]$ یک تکریختی حلقه‌هاست. به همین نحو، به‌ازای هر زیرمجموعهٔ $\{i_1, \ldots, i_k\}$ از $\{1,2, \ldots, n\}$، یک تکریختی مانند $R[x_{i_1}, \ldots, x_{i_k}] \to R[x_1, \ldots, x_n]$ وجود دارد. $R[x_{i_1}, \ldots, x_{i_k}]$ را معمولاً " با نقش یکریخت خود یکی کرده و آن را یک زیرحلقهٔ $R[x_1, \ldots, x_n]$ درنظر می‌گیریم.

فرض کنیم $\varphi : R \to S$ یک همریختی حلقه‌ها بوده، $f \in R[x_1, \ldots, x_n]$، و $s_1, s_2, \ldots, s_n \in S$. بنابر قضیهٔ ۴۰۵، $f = \sum_{i=0}^{m} a_ix_1^{k_{i1}}\cdots x_n^{k_{in}}$ که در آن $a_i \in R$ و $k_{ij} \in \mathbf{N}$.

تمام x_i هایی کـه نمای صفر دارند را حذف می‌کنیم . در این صورت ، $\varphi f(s_1,s_2,\ldots,s_n)$ مساوی $\sum_{i=0}^{m}\varphi(a_i)s_1^{k_{i1}}\cdots s_n^{k_{in}}\in S$ تعریف شده است؛ یعنی ، $\varphi f(s_1,\ldots,s_n)$ با گذاردن $\varphi(a_i)$ به جای a_i و $s_i^{k_{ij}}$ به جای $x_i^{k_{ij}}$ $(k_{ij}>0)$ به‌دست می‌آید . چون a_i و k_{ij} به‌طور منحصر به فـرد معین می‌شوند (قضیهٔ ۴۰۵) ، $\varphi f(s_1,\ldots,s_n)$ یک عنصر تعریف شدهٔ S است . اگر R یک زیرحلقهٔ S بوده و φ نگاشت شمول باشد ، به جای $\varphi f(s_1,\ldots,s_n)$ می‌نویسیم $f(s_1,\ldots,s_n)$.

همانند بسیاری از جـالبترین ساختهای جبری ، حلقهٔ چندجمله‌ای $R[x_1,\ldots,x_n]$ را می‌توان با خـاصیت نگاشت عمومی مشخص کرد . اگر مفروضات مناسبی افزوده شوند ، قضیهٔ زیر و نتایج آن در حالت غیرتعویضپذیر درستنـــد (تمرین ۵) . اینهـــا بـــرای حلقه‌های چندجمله‌ایها با تعداد نامتناهی مجهول نیز درستند (تمرین ۴) .

قضیهٔ ۵۰۵ . فرض کنیم R و S حلقه‌های تعویضپذیر یکـداری بوده و $\varphi : R \to S$ یک همـریختی حلقـه‌ها باشد به‌طوری‌که $\varphi(1_R) = 1_S$. هـرگاه $s_1,s_2,\ldots,s_n \in S$ ، آنگاه یک همریختی منحصر به فـرد از حلقه‌ها مانند $\bar{\varphi} : R[x_1,\ldots,x_n] \to S$ وجوددارد به‌طوری‌که $\bar{\varphi} \mid R = \varphi$ و ، به‌ازای $i = 1,2,\ldots,n$ ، $\bar{\varphi}(x_i) = s_i$. ایـن خاصیت حلقهٔ چندجمله‌ای $R[x_1,\ldots,x_n]$ را کاملا " با تقریب یکریختی معین می‌کند .

طرح برهان . هرگاه $f \in R[x_1,\ldots,x_n]$ ، آنگاه ، طبق قضیهٔ ۴۰۵ ،

$$f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}} \quad (a_i \in R; k_{ij} \in \mathbf{N}).$$

نگاشت $\bar{\varphi}$ داده شـده بـا $\bar{\varphi}(f) = \varphi f(s_1,\ldots,s_n)$ بوضوح یک نگاشت تعریف شده است به طوری که $\bar{\varphi} \mid R = \varphi$ و $\bar{\varphi}(x_i) = s_i$. با استفاده از همریختی بودن φ ، قواعد نماگیری ، و قضیـهٔ دوجملـه‌ای ۶۰۱ ، تحقیق کنید که $\bar{\varphi}$ یک همـریختی حلقـه‌هاست . فرض کنید $\psi : R[x_1,\ldots,x_n] \to S$ یک همـریختی بـاشد بـه‌طوری که $\psi \mid R = \varphi$ و ، به‌ازای هر i ، $\psi(x_i) = s_i$. در این صورت ،

$$\psi(f) = \psi\left(\sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}}\right) = \sum_{i=0}^{m} \psi(a_i)\psi(x_1^{k_{i1}}) \cdots \psi(x_n^{k_{in}})$$

$$= \sum_{i=0}^{m} \varphi(a_i)\psi(x_1)^{ki1} \cdots \psi(x_n)^{kin}$$

$$= \sum_{i=0}^{m} \varphi(a_i)s_1^{ki1} \cdots s_n^{kin} = \varphi f(s_1, s_2, \ldots, s_n) = \bar{\varphi}(f);$$

که از آنجا $\bar{\varphi} = \psi$ و $\bar{\varphi}$ منحصربه‌فرداست. بالاخره، برای آنکه نشان دهیم $R[x_1, \ldots, x_n]$ کاملا" با این خاصیت نگاشت معین می‌شود، رستهٔ $\mathcal{C}$ را تعریف می‌کنیم که اشیاء آن تمام $(n+2)$ تاییهای $(\psi, K, s_1, \ldots, s_n)$ هستند، که در آنها K یک حلقهٔ تعویضپذیر یکدار است، $s_i \in K$، و $\psi : R \to K$ یک همریختی با $\psi(1_R) = 1_K$ می‌باشد. یک ریخت در $\mathcal{C}$ از $(\psi, K, s_1, \ldots, s_n)$ به $(\theta, T, t_1, \ldots, t_n)$ یک همریختی حلقه‌ها مانند $\zeta : K \to T$ است به‌طوری‌که $\zeta(1_K) = 1_T$، $\zeta\psi = \theta$ و، به‌ازای $i = 1, 2, \ldots, n$، $\zeta(s_i) = t_i$. تحقیق کنید که ζ یک تعادل در $\mathcal{C}$ است اگروفقط اگر ζ یک‌یکریختی حلقه‌ها باشد. هرگاه $\iota : R \to R[x_1, \ldots, x_n]$ یک‌نگاشت شمول باشد، آنگاه قسمت اول برهان نشان می‌دهد که $(\iota, R[x_1, \ldots, x_n], x_1, \ldots, x_n)$ یک شیٔ عمومی در $\mathcal{C}$ است. بنابراین، طبق قضیهٔ ۱ ۰۷۰ ۱۰، $R[x_1, \ldots, x_n]$ کاملا" با تقریب یکریختی معین می‌شود.

نتیجهٔ ۶۰۵. **هرگاه $\varphi : R \to S$ یک همریختی حلقه‌های تعویضپذیر بوده و $s_1, s_2, \ldots, s_n \in S$، آنگاه نگاشت $R[x_1, \ldots, x_n] \to S$ داده شده با $f \mapsto \varphi f(s_1, \ldots, s_n)$ یک همریختی حلقه‌ها می‌باشد.**

طرح برهان ۶۰۵. برهان قضیهٔ ۵۰۵ نشان می‌دهد که انتساب $f \mapsto \varphi f(s_1, \ldots, s_n)$ یک همریختی تعریف می‌کند که حتی وقتی R و S دارای واحد نیز نباشند معتبر است.

چند تبصره. نگاشت $R[x_1, \ldots, x_n] \to S$ درنتیجهٔ ۶۰۵ ***ارزیابی یا همریختی جانشانی*** نام دارد. اگر R و S تعویضپذیر نباشند، نتیجهٔ ۶۰۵ ممکن است درست نباشد. این امر مهم است، زیرا نتیجهٔ ۶۰۵ بارها بدون ذکر صریح به‌کار می‌رود. مثلا"، این استدلال که هرگاه $f = gh$ $(f, g, h \in R[x])$ و $c \in R$، آنگاه $f(c) = g(c)h(c)$، ممکن است در صورت تعویضپذیر نبودن R برقرار نباشد (تمرین ۶).

نتیجهٔ دیگر قضیهٔ ۵۰۵ را می‌توان با مثال زیر توضیح داد. فرض کنیم R یک حلقهٔ تعویضپذیر یکدار بوده و چندجمله‌ای

$$f = x^2y + x^3y + x^4 + xy + y^2 + r \in R[x,y]$$

را درنظر می‌گیریم . توجه کنید که $f = y^2 + (x^2 + x^3 + x)y + (x^4 + r)$ ، که از آنجا $f \in R[x][y]$. به همین نحو ، $f = x^4 + yx^3 + yx^2 + yx + (y^2 + r) \in R[y][x]$. این پیشنهاد می‌کند که $R[x,y]$ با هر دوی $R[x][y]$ و $R[y][x]$ یکریخت‌است . به‌طورکلی ، داریم

نتیجهٔ ۷۰۵ . فرض کنیم R یک حلقهٔ تعویضپذیر یکدار بوده و n عدد صحیح مثبتی باشد . به‌ازای هر $(1 \leq k < n)$ k ، یکریختیهایی از حلقه‌ها مانند $R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] \cong R[x_1, \ldots, x_n] \cong R[x_{k+1}, \ldots, x_n][x_1, \ldots, x_k]$ وجود دارند .

برهان . نتیجه را می‌توان مستقیما" با ساختن یکریختیها یا با استفاده از خاصیت نگاشت عمومی قضیهٔ ۵۰۵ به صورت زیر ثابت کرد . بنابر قضیهٔ ۵۰۵ ، به‌ازای همریختی $\varphi : R \to S$ از حلقه‌های تعویضپذیر یکدار و عناصر $s_1, \ldots, s_n \in S$ ، یک همریختی مانند $\bar{\varphi} : R[x_1, \ldots, x_k] \to S$ وجود دارد به‌طوری‌که $\bar{\varphi} \mid R = \varphi$ و ، به‌ازای $i = 1,2, \ldots, k$ ، $\bar{\varphi}(x_i) = s_i$. با اعمال قضیهٔ ۵۰۵ با $R[x_1, \ldots, x_k]$ به جای R ، همریختی $\bar{\bar{\varphi}} : R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] \to S$ به دست می‌آید به‌طوری‌که $\bar{\bar{\varphi}} \mid R[x_1, \ldots, x_k] = \bar{\varphi}$ و ، به‌ازای $i = k+1, \ldots, n$ ، $\bar{\bar{\varphi}}(x_i) = s_i$. بنابرساخت ، $\bar{\bar{\varphi}} \mid R = \bar{\varphi} \mid R = \varphi$ و ، به‌ازای $i = 1,2, \ldots, n$ ، $\bar{\bar{\varphi}}(x_i) = s_i$. فرض کنیم $\psi : R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] \to S$ یک همریختی باشد به‌طوری که $\psi \mid R = \varphi$ و ، به‌ازای $i = 1,2, \ldots, n$ ، $\psi(x_i) = s_i$. در این صورت ، همان استدلال به کار رفته در برهان یکتایی قضیهٔ ۵۰۵ نشان می‌دهد که $\psi \mid R[x_1, \ldots, x_k] = \bar{\varphi}$. بنابراین ، حکم یکتایی قضیهٔ ۵۰۵ (اعمال شده بر $R[x_1, \ldots, x_k]$) ایجاب می‌کند که $\psi = \bar{\bar{\varphi}}$. درنتیجه ، $R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n]$ دارای خاصیت نگاشت عمومی‌است ، که‌ازآنجا ، طبق قضیهٔ ۵۰۵ ، $R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] \cong R[x_1, \ldots, x_n]$. یکریختی دیگر نیز به همین نحو ثابت می‌شود .

چون $R[x_1, \ldots, x_k]$ معمولا" زیرحلقهٔ $R[x_1, \ldots, x_n]$ گرفته می‌شود (ر . ک . صفحهٔ ۲۳۷) ، معمولا" حلقه‌های چندجمله‌ای مختلف درنتیجهٔ ۶۰۵ را تحت یکریختیهای مذکوردرآنجایکی کرده‌و ، مثلا" ، می‌نویسند $R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n] = R[x_1, \ldots, x_n]$.

این بخش را با مقدمهٔ کوتاهی در باب سریهای توانی صوری ، که در آینده لازم

نمی‌شود ، به‌پایان می‌بریم .

حکم ۸۰۵ . *فرض کنیم* R *حلقه بوده و* $R[[x]]$ *مجموعهٔ تمام دنباله‌ها از عناصر مانند* $(a_0,a_1,\ldots)$ *از عناصر* R *باشد .*

(یک) $R[[x]]$ *با جمع و ضربی که به صورت زیر تعریف شده‌اند یک حلقه است :*

$$(a_0,a_1,\ldots)+(b_0,b_1,\ldots)=(a_0+b_0,a_1+b_1,\ldots)$$

و

$$(a_0,a_1,\ldots)(b_0,b_1,\ldots)=(c_0,c_1,\ldots)$$

که

$$c_n=\sum_{i=0}^{n}a_ib_{n-i}=\sum_{k+j=n}a_kb_j\ .$$

(دو) *حلقهٔ چندجمله‌ای* $R[x]$ *یک زیرحلقهٔ* $R[[x]]$ *است .*

(سه) *هرگاه* R *تعویضپذیر [یا حلقه‌ای یکدار یا حلقه‌ای بدون مقسوم‌علیه صفر یا دامنهٔ صحیح] باشد ، آنگاه* $R[[x]]$ *نیز چنین است .*

برهان . تمرین ؛ ر.ک. قضیهٔ ۱۰۵ .

حلقهٔ $R[[x]]$ حکم ۸۰۵ **حلقهٔ سریهای توانی صوری** روی حلقهٔ R نام دارد . عنصرهایش **سریهای توانی** نامیده می‌شوند . هرگاه R یکدار باشد ، آنگاه چندجمله‌ای $x=(0,1_R,0,\ldots)\in R[[x]]$ یک **مجهول** نامیده می‌شود . به آسانی معلوم می‌شود که به‌ازای هر $r\in R$ و $i\in\mathbf{N}$ ، $x^ir=rx^i$ ، هرگاه $(a_0,a_1,\ldots)\in R[[x]]$ ، آنگاه به‌ازای هر n ، $(a_0,a_1,\ldots,a_n,0,0,\ldots)$ یک چندجمله‌ای است ، که از آنجا ، طبق قضیهٔ ۲۰۵ ، $(a_0,\ldots,a_n,0,0,\ldots)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$. در نتیجه ، می‌توان نماد زیر را پذیرفت . سری توانی $(a_0,a_1,\ldots)\in R[[x]]$ با مجموع صوری $\sum_{i=0}^{\infty}a_ix^i$ نموده می‌شود . عناصر a_i **ضرایب** و a_0 **جملهٔ ثابت** نام دارند . این نماد ، مثل چندجمله‌ایها ، حتی وقتی R یکدار نیست (که در این صورت $x\notin R[[x]]$) به کار می‌رود .

حکم ۹۰۵ . *فرض کنیم* R *حلقه‌ای یکدار بوده و* $f=\sum_{i=0}^{\infty}a_ix^i\in R[[x]]$.

(یک) f **یک یکه در** $R[[x]]$ **است اگر و فقط اگر جملهٔ ثابت آن** a_0 **یک یکه در** R **باشد.**
(دو) هرگاه a_0 **در** R **تحویل‌ناپذیر باشد، آنگاه** f **در** $R[[x]]$ **تحویل‌ناپذیر می‌باشد.**

تبصره. هرگاه $f \in R[[x]]$ یک چندجمله‌ای با جملهٔ ثابت تحویل‌ناپذیر [یا یکه] باشد، آنگاه f در حلقهٔ چندجمله‌ای $R[x]$ لزوماً تحویل‌ناپذیر [یا یکه] نیست (تمرین ۸).

برهان ۹۰۵. (یک) اگر $g = \sum b_i x^i \in R[[x]]$ ای موجود باشد به‌طوری‌که

$$fg = gf = 1_R \in R[[x]],$$

فوراً نتیجه می‌شود که $a_0 b_0 = b_0 a_0 = 1_R$، که‌ازآنجا a_0 در R یکه‌است. حال فرض کنیم a_0 در R یکه‌باشد. هرگاه عنصری چون $g = \sum b_i x^i \in R[[x]]$ وجود می‌داشت که $fg = 1_R$، آنگاه معادلات زیر برقرار بودند:

$$\begin{aligned} a_0 b_0 &= 1_R \\ a_0 b_1 + a_1 b_0 &= 0 \\ &\vdots \\ a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 &= 0 \\ &\vdots \end{aligned}$$

به عکس، هرگاه جواب $(b_0, b_1, b_2, \ldots)$ این دستگاه معادلات در R وجود داشته باشد، آنگاه $g = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ بوضوح دارای خاصیت $fg = 1_R$ است. چون a_0 یکه (با معکوس ضربی a_0^{-1}) است، معادلهٔ اول را می‌شود حل کرد: $b_0 = a_0^{-1}$: به همین نحو، $b_1 = a_0^{-1}(-a_1 b_0) = a_0^{-1}(-a_1 a_0^{-1})$. به استقرا عمل می‌کنیم؛ هرگاه $b_0, \ldots, b_{n-1}$ برحسب a_i ها معین شده باشند، آنگاه $a_0 b_n = -a_1 b_{n-1} - \cdots - a_n b_0$ ایجاب می‌کند که $b_n = a_0^{-1}(-a_1 b_{n-1} - \cdots - a_n b_0)$. لذا، اگر a_0 یکه‌باشد، این دستگاه معادلات را می‌توان حل کرد و g ای وجودخواهدداشت به‌طوری که $fg = 1_R \in R[[x]]$. استدلالی مشابه نشان می‌دهد که $h \in R[[x]]$ ی وجود دارد به‌طوری‌که $hf = 1_R$. اما $h = h1_R = h(fg) = (hf)g = 1_R g = g$، که از آنجا g یک معکوس دوطرفهٔ f می‌شود. بنابراین، f یک یکه در $R[[x]]$ می‌باشد. قسمت (دو) نتیجه‌ای فوری از قسمت (یک)

است .

نتیجهٔ ۱۰.۵ . هرگاه R یک حلقهٔ بخشی باشد ، آنگاه یکه‌های موجود در R[[x]] درست آن سریهای توانی هستند که جملهٔ ثابت آنها ناصفر است . ایده‌آل اصلی (x) درست از غیریکه‌ها در R[[x]] تشکیل شده است و ایده‌آل ماکزیمال منحصر به فرد R[[x]] می‌باشد . لذا ، اگر R میدان باشد ، R[[x]] یک حلقهٔ موضعی می‌شود .

برهان . حکم اول از حکم ۹.۵ (یک) و اینکه هر عنصر ناصفر R یکه است نتیجه می‌شود. چون x در مرکز $R[[x]]$ است ، طبق قضیهٔ ۵.۲ ،

$$(x) = \{xf \mid f \in R[[x]]\}$$

درنتیجه ، هر عنصر xf از (x) دارای جملهٔ ثابت صفر است ، که از آنجا xf یک غیریکه است . به‌عکس ، هرغیریکهٔ $f \in R[[x]]$ لزوماً به شکل $f = \sum_{i=0}^{\infty} a_i x^i$ است که در آن $a_0 = 0$. فرض کنیم $g = \sum_{i=0}^{\infty} b_i x^i$ ، که در آن به‌ازای هر i ، $b_i = a_{i+1}$. در این صورت $xg = f$ که از آنجا $f \in (x)$. بنابراین ، (x) مجموعهٔ غیریکه‌هاست . بالاخره ، چون $1_R \notin (x)$ ، $(x) \neq R[[x]]$. به علاوه ، هر ایده‌آل I از $R[[x]]$ که $I \neq R[[x]]$ لزوماً از غیریکه‌ها تشکیل شده است (تبصره‌های ص ۱۹۰) . لذا ، هر ایده‌آل $R[[x]]$ جز $R[[x]]$ مشمول (x) می‌باشد . بنابراین ، (x) ایده‌آل ماکزیمال منحصر به فرد $R[[x]]$ می‌باشد .

تمرینات

۱ . (آ) هرگاه $\varphi : R \to S$ یک‌همریختی حلقه‌ها باشد ، آنگاه نگاشت $\bar{\varphi} : R[[x]] \to S[[x]]$ داده شده با $\bar{\varphi}(\sum a_i x^i) = \sum \varphi(a_i) x^i$ یک همریختی حلقه‌هاست به‌طوری‌که $\bar{\varphi}(R[x]) \subset S[x]$.

(ب) $\bar{\varphi}$ یک تکریختی [برووریختی] است اگرو فقط اگر φ چنین باشد . در این حالت $\bar{\varphi} : R[x] \to S[x]$ نیز یک تکریختی [برووریختی] می‌باشد .

(پ) نتایج (آ) و (ب) را به حلقه‌های چندجمله‌ای $R[x_1, \ldots, x_n]$, $S[x_1, \ldots, x_n]$ تعمیم دهید .

۲ . فرض کنید $\mathrm{Mat}_n R$ حلقهٔ ماتریسهای $n \times n$ روی حلقهٔ R باشد . در این صورت ،

به‌ازای هر $n \geq 1$ ،

(آ) $(\mathrm{Mat}_n R)[x] \cong \mathrm{Mat}_n R[x]$ ؛

(ب) $(\mathrm{Mat}_n R)[[x]] \cong \mathrm{Mat}_n R[[x]]$.

۳ . فرض کنید R یک‌حلقه‌و G یک‌گروه دوری‌ضربی‌نامتناهی‌با مولد x باشد . آیاحلقهٔ گروهی $R(G)$ (ر.ک. صفحهٔ ۱۸۱) با حلقهٔ چندجمله‌ای یک مجهولی روی R یکریخت است؟

۴ . (آ) فرض‌کنید S یک‌مجموعهٔ‌ناتهی بوده و $\mathbf{N}^S$ مجموعهٔ تمام توابع $\varphi : S \to \mathbf{N}$ باشد به‌طوری‌که در حداکثر تعدادی متناهی عنصر $s \in S$ داشته باشیم $\varphi(s) \neq 0$. دراین‌صورت ، $\mathbf{N}^S$ یک تکگون آبلی **ضربی** است که در آن ضرب به صورت زیرتعریف می‌شود :

$$(\varphi\psi)(s) = \varphi(s) + \psi(s) \quad (\varphi,\psi \in \mathbf{N}^S; s \in S).$$

عنصر همانی در $\mathbf{N}^S$ تابع صفر است .

(ب) فرض‌کنید $x^i \in \mathbf{N}^S$ ، به‌ازای هر $x \in S$ و $i \in \mathbf{N}$ ، با $x^i(x) = i$ و ، به‌ازای $s \neq x$ ، با $x^i(s) = 0$ تعریف‌شده‌باشد . هرگاه $\varphi \in \mathbf{N}^S$ و $x_1, \ldots, x_n$ تنها عناصری از S باشد که $\varphi(x_i) \neq 0$ ، آنگاه ، در $\mathbf{N}^S$ ، $\varphi = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ ، که در آن $i_j = \varphi(x_j)$.

(پ) اگر R یک حلقهٔ یکدار باشد ، $R[S]$ را مجموعهٔ تمام توابع $f : \mathbf{N}^S \to R$ بگیرید که به‌ازای حداکثر تعدادی متناهی $\varphi \in \mathbf{N}^S$ ، $f(\varphi) \neq 0$. در این صورت ، $R[S]$ حلقه‌ای یکدار است ، که در آن جمع و ضرب به صورت زیر تعریف می‌شوند :

$$(f+g)(\varphi) = f(\varphi) + g(\varphi) \quad (f,g \in R[S]; \varphi \in \mathbf{N}^S);$$
$$(fg)(\varphi) = \sum f(\theta)g(\zeta) \quad (f,g \in R[S]; \theta,\zeta,\varphi \in \mathbf{N}^S),$$

که در آنها مجموع روی تمام جفتهای (θ,ζ) گرفته می‌شود که $\theta\zeta = \varphi$. $R[S]$ **حلقهٔ چندجمله‌ایها در S روی R** نام دارد .

(ت) به‌ازای هر $\varphi = x_1^{i_1} \cdots x_n^{i_n} \in \mathbf{N}^S$ و هر $r \in R$ ، $rx_1^{i_1} \cdots x_n^{i_n}$ تابعی است مانند $\mathbf{N}^S \to R$ که در φ مساوی r و جاهای دیگر 0 است . در این صورت ، هرعنصر ناصفر f از $R[S]$ را می‌توان به شکل $f = \sum_{i=0}^{m} r_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$ نوشت ، که در آن $r_i \in R, x_i \in S$ و همهٔ $k_{ij} \in \mathbf{N}$ ها به‌طور منحصر به فرد معین می‌شوند .

(ث) هرگاه S متناهی و با اصلیت n باشد، آنگاه $R[S] \cong R[x_1, \ldots, x_n]$.
[**راهنمایی.** هرگاه $\mathbf{N}^n$ یک تکگون آبلی جمعی همانند در متن گرفته شود، آنگاه یک یکریختی تکگونها مانند $\mathbf{N}^S \cong \mathbf{N}^n$ وجود داردکه با $\varphi \mapsto (\varphi(s_1), \ldots, \varphi(s_n))$ داده می‌شود، که در آن $S = \{s_1, \ldots, s_n\}$.]

(ج) مشابه قضیهٔ ۵۰۵ را برای $R[S]$ بیان و اثبات کنید.

۵. فرض کنید R و S حلقه‌هایی یکدار بوده، $\varphi : R \to S$ یک همریختی حلقه‌ها باشد که $\varphi(1_R) = 1_S$، و $s_1, s_2, \ldots, s_n \in S$ چنان باشند که به‌ازای هر i,j، $s_i s_j = s_j s_i$ و به‌ازای هر $r \in R$ و هر i، $\varphi(r)s_i = s_i\varphi(r)$. در این‌صورت، یک همریختی منحصر به فرد، مانند $\bar{\varphi} : R[x_1, \ldots, x_n] \to S$ وجود دارد به‌طوری‌که $\bar{\varphi}|R = \varphi$ و $\bar{\varphi}(x_i) = s_i$. این خاصیت $R[x_1, \ldots, x_n]$ را کاملا" با تقریب یکریختی معین خواهد کرد.

۶. (آ) هرگاه R حلقهٔ تمام ماتریسهای 2×2 روی $\mathbf{Z}$ باشد، آنگاه به‌ازای هر $A \in R$،

$$(x + A)(x - A) = x^2 - A^2 \in R[x].$$

(ب) $C, A \in R$ ای وجود دارند به‌طوری‌که $(C + A)(C - A) \neq C^2 - A^2$. بنابراین، نتیجهٔ ۶۰۵ در صورت تعویض‌ناپذیر بودن حلقه‌ها درست نیست.

۷. هرگاه R یک حلقهٔ تعویضپذیر یکدار بوده و $f = a_n x^n + \cdots + a_0$ یک مقسوم‌علیه صفر در $R[x]$ باشد، آنگاه عنصر ناصفری مانند $b \in R$ وجود دارد به‌طوری‌که $ba_n = ba_{n-1} = \cdots = ba_0 = 0$.

۸. (آ) چندجمله‌ای $x + 1$ در حلقهٔ سریهای توانی $\mathbf{Z}[[x]]$ یکه است، ولی در $\mathbf{Z}[x]$ یکه نیست.

(ب) $x^2 + 3x + 2$ در $\mathbf{Z}[[x]]$ تحویل‌ناپذیر است، ولی در $\mathbf{Z}[x]$ چنین نیست.

۹. هرگاه F یک میدان باشد، آنگاه (x) یک ایده‌آل ماکزیمال در $F[x]$ است، ولی تنها ایده‌آل ماکزیمال نیست (با نتیجهٔ ۱۰۰۵ مقایسه کنید).

۱۰. (آ) هرگاه F یک‌میدان باشد، آنگاه هر عنصر ناصفر $F[[x]]$ به‌شکل $x^k u$ است‌که $u \in F[[x]]$ یکه می‌باشد.

(ب) $F[[x]]$ یک دامنهٔ ایده‌آل اصلی است که تنها ایده‌آلهای آن عبارتند از 0، $F[[x]] = (1_F) = (x^0)$، و (x^k) به‌ازای هر $k \geq 1$.

۱۱. فرض کنید $\mathfrak{C}$ رسته‌ای باشد که اشیاء آن تمام حلقه‌های تعویضپذیر یکدار بوده و ریختهایش تمام همریختیهای حلقه‌ها مانند $f : R \to S$ باشند به‌طوری‌که $f(1_R) = 1_S$.

در ایـن صـورت، حلقهٔ چندجمله‌ایهای $\mathbf{Z}[x_1, \ldots, x_n]$ یک شیٔ آزاد بر مجموعهٔ $\{x_1, \ldots, x_n\}$ در رستهٔ $\mathcal{C}$ است. [**راهنمایی.** به‌ازای هـر R در $\mathcal{C}$، نگاشت $\mathbf{Z} \to R$ داده شـده با $n \mapsto n1_R$ یک همریختی حلقه‌هاست؛ از قضیهٔ ۵۰۵ استفاده کنید.]

۶ تجزیه در حلقه‌های چندجمله‌ای

حال به مباحث بـخش ۳ (بخشپذیری، تحویل‌ناپذیری، و یکتایی تجزیه) در محدودهٔ حلقه‌های چندجمله‌ای روی یک حلقهٔ تعویضپذیر می‌پردازیم. بحث را با دو ابزار اساسی زیرآغاز می‌کنیم: مفهوم درجهٔ یک‌چندجمله‌ای و الگوریتم تقسیم. سپس عوامل درجهٔ یک چندجمله‌ای را مطالعه می‌نماییم؛ یافتن این عاملها معادل یافتن ریشه‌های چندجمله‌ای است. بـالاخره، عـوامل تحـویل‌ناپذیر از درجـهٔ بـالاتر را درنظر می‌گیریم: محک تحویل‌ناپذیری آیزنشتاین[1] را ثابت کرده و نشان می‌دهیم که دامنهٔ چندجمله‌ای $D[x_1, \ldots, x_n]$ یک دامنهٔ یکتایی تجزیه است اگر D چنین باشد.

فرض کنیم R یک‌حلقه‌باشد. **درجهٔ تکجمله‌ای ناصفر** $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \in R[x_1, \ldots, x_n]$ عـدد صحیـح نامنفی $k_1 + k_2 + \cdots + k_n$ اسـت. هـرگاه f یک چندجمله‌ای ناصفر در $R[x_1, \ldots, x_n]$ باشد، آنـگاه، بنابر قضیهٔ ۴۰۵، $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}}$. **درجهٔ (کل) چندجمله‌ای** f ماکزیمـم درجـات تکجمله‌ایهای $a_i x_1^{k_{i1}}, \ldots, x_n^{k_{in}}$ است به‌طوری‌که $a_i \neq 0$ $(i = 1,2, \ldots, m)$. درجهٔ (کل) f با $\deg f$ نموده می‌شود. واضح است که چندجمله‌ای ناصفر f دارای درجهٔ صفر است اگر و فقط اگر f چندجمله‌ای ثابت $f = a_0 = a_0 x_1^0 \cdots x_n^0$ باشد. یـک چنـدجمله‌ای که مجموعی از تکجمله‌ایهاست و هر یک از درجهٔ k می‌باشد، **همگـن از درجـهٔ k** نامیـده مـی‌شود. به یاد آورید که به‌ازای هر k $(1 \leq k \leq n)$، $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ یک زیـرحلقهٔ $R[x_1, \ldots, x_n]$ است (ر.ک. صفحهٔ ۲۳۷). **درجهٔ f در x_k** درجهٔ f به عنـوان یـک چنـدجمله‌ای از مجهـول x_k روی حلقـهٔ $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ است.

مثال. چندجمله‌ای $3x_1^2x_2^2x_3^2 + 3x_1x_3^4 - 6x_2^3x_3 \in \mathbf{Z}[x]$ نسبت‌به x_1 ازدرجهٔ 2، نسبت به x_2 از درجهٔ 3، نسبت به x_3 از درجهٔ 4 بوده، و درجهٔ کل آن 6 است.

1. Eisenstein

به دلایل تکنیکی، شایسته است درجهٔ چندجمله‌ای صفر مساوی $-\infty$ تعریف شده و قراردادهای زیر در باب علامت $\deg 0 = -\infty$ پذیرفته‌شود: به‌ازای هر عدد صحیح n، $n < -\infty$ و $n + (-\infty) = -\infty + n = -\infty$؛ $(-\infty) + (-\infty) = -\infty$.

قضیهٔ ۱۰۶. فرض کنیم R حلقه بوده و $f,g \in R[x_1, \ldots, x_n]$.

(یک) $\deg(f+g) \leq \max(\deg f, \deg g)$.

(دو) $\deg(fg) \leq \deg f + \deg g$.

(سه) اگر R مقسوم‌علیه صفر نداشته باشد، $\deg(fg) = \deg f + \deg g$.

(چهار) هرگاه $n = 1$ و ضریب‌پیشرو f یا g یک‌مقسوم‌علیه‌صفردر R نباشد (بخصوص، اگر یکه باشد)، آنگاه $\deg(fg) = \deg f + \deg g$.

تبصره. قضیه درصورتی که $\deg f$ به معنی "درجهٔ f نسبت به x_k" گرفته شود نیز درست است.

طرح برهان ۱۰۶. چون این قضیه عمدتاً به‌ازای $n = 1$ به کار می‌رود، فقط آن را در این‌حالت ثابت می‌کنیم. قسمت (یک) آسان است. اگر $f = 0$ یا $g = 0$، قسمت (دو) بدیهی است. هرگاه $f = \sum_{i=0}^{n} a_i x^i \neq 0$ دارای درجهٔ n بوده‌و $g = \sum_{i=0}^{m} b_i x^i \neq 0$ دارای درجهٔ m باشد، آنگاه

$$fg = a_0 b_0 + \cdots + (a_{n-1}b_m + a_n b_{m-1})x^{n+m-1} + a_n b_m x^{m+n}$$

دارای درجهٔ حداکثر $m+n$ است. چون $a_n \neq 0 \neq b_m$، اگر یکی از a_n, b_m مقسوم‌علیه صفر نباشد، fg دارای درجهٔ $m+n$ می‌باشد.

قضیهٔ ۲۰۶ (الگوریتم تقسیم). فرض کنیم R حلقه‌ای یکدار بوده و $f,g \in R[x]$ چندجمله‌ایهای ناصفری باشند به‌طوری‌که ضریب پیشرو g یک یکه در R باشد. در این صورت، چندجمله‌ایهای منحصر به فردی مانند $q,r \in R[x]$ وجود دارند به‌طوری‌که

$$f = qg + r \quad \text{و} \quad \deg r < \deg g.$$

برهان. اگر $\deg g > \deg f$ ، قرار می‌دهیم $q = 0$ و $r = f$. هرگاه $\deg g \leq \deg f$ ، آنگاه $f = \sum_{i=0}^{n} a_i x^i$ ، $g = \sum_{i=0}^{m} b_i x^i$ ، که در آنها $a_n \neq 0$ ، $b_m \neq 0$ ، $m \leq n$ ، و b_m یک یکه در R است . بـه استقـرا بر $n = \deg f$ عمل مـی‌کنیم . هرگاه $n = 0$ ، آنگاه $m = 0$ ، $f = a_0$ ، $g = b_0$ ، و b_0 یکه است . فرض کنیم $q = a_0 b_0^{-1}$ و $r = 0$ ؛ در ایـن صورت ، $qg + r = (a_0 b_0^{-1}) b_0 = a_0 = f$ و $\deg r < \deg g$.

فرض کنیم قسمت وجودی قضیه برای چندجمله‌ایهای از درجهٔ کمتر از $n = \deg f$ درست‌باشد . محاسبه‌ای مستقیم نشان می‌دهد که چندجمله‌ای $(a_n b_m^{-1} x^{n-m})g$ دارای درجهٔ n و ضریب پیشرو a_n است . از اینرو ،

$$f - (a_n b_m^{-1} x^{n-m})g = (a_n x^n + \cdots + a_0) - (a_n x^n + \cdots + a_n b_m^{-1} b_0 x^{n-m})$$

یک چندجمله‌ای از درجهٔ کمتر از n است . بنابه فرض استقرا ، چندجمله‌ایهایی مانند q' و r وجود دارند به‌طوری‌که

$$f - (a_n b_m^{-1} x^{n-m})g = q'g + r \quad \text{و} \quad \deg r < \deg g .$$

بنابراین ، هرگاه $q = a_n b_m^{-1} x^{n-m} + q'$ ، آنگاه

$$f = (a_n b_m^{-1} x^{n-m})g + q'g + r = qg + r.$$

(یکتـایی) . فـرض کنیم $f = q_1 g + r_1$ و $f = q_2 g + r_2$ که در آنـها $\deg r_1 < \deg g$ و $\deg r_2 < \deg g$. در این صورت ، $q_1 g + r_1 = q_2 g + r_2$ ایجاب می‌کند که

$$(q_1 - q_2)g = r_2 - r_1.$$

چون ضریب پیشرو b_m از g یک یکه است ، قضیهٔ ۶.۱ ایجاب می‌کند که

$$\deg (q_1 - q_2) + \deg g = \deg (q_1 - q_2)g = \deg(r_2 - r_1).$$

چون $\deg(r_2 - r_1) \leq \max (\deg r_2, \deg r_1) < \deg g$ ، تساوی فوق درسـت است فقط اگر $\deg(q_1 - q_2) = (-\infty) = \deg(r_2 - r_1)$. به عبارت دیگر ، $q_1 - q_2 = 0$ و $r_2 - r_1 = 0$.

نتیجهٔ ۳.۶ (قضیهٔ باقیمانده) . *فرض کنیم R حلقه‌ای یکدار بوده و*

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x].$$

بـه‌ازای هـر $c \in R$ ، یـک $q(x) \in R[x]$ منحصـر بـه فـرد وجـود دارد به‌طوری‌که

$$f(x) = q(x)(x - c) + f(c) .$$

برهان. اگر $f = 0$ ، قرار می‌دهیم $q = 0$. پس فرض کنیم $f \neq 0$. قضیهٔ ۲۰۶ ایجاب می‌کند که چندجمله‌ایهای منحصر به فردی مانند $q(x), r(x)$ در $R[x]$ وجود داشته باشند به‌طوری‌که $f(x) = q(x)(x - c) + r(x)$ و $\deg r(x) < \deg (x - c) = 1$. لذا ، $r(x) = r$ یک چندجمله‌ای ثابت (احتمالاً " 0 ") است . هرگاه $q(x) = \sum_{j=0}^{n-1} b_j x^j$ ، آنگاه

$$f(x) = q(x)(x - c) + r = -b_0 c + \sum_{k=1}^{n-1} (-b_k c + b_{k-1})x^k + b_{n-1}x^n + r ,$$ که از آنجا

$$\begin{aligned} f(c) &= -b_0 c + \sum_{k=1}^{n-1} (-b_k c + b_{k-1})c^k + b_{n-1}c^n + r \\ &= -\sum_{k=0}^{n-1} b_k c^{k+1} + \sum_{k=1}^{n} b_{k-1}c^k + r = 0 + r = r . \end{aligned}$$

نتیجهٔ ۴۰۶ . هرگاه F یک میدان باشد ، آنگاه حلقهٔ چندجمله‌ای F[x] یک دامنهٔ اقلیدسی است ، که از آنجا F[x] یک دامنهٔ ایده‌آل اصلی و یک دامنهٔ یکتایی تجزیه است . یکه‌های موجود در F[x] درست چندجمله‌ایهای ثابت ناصفرند .

طرح برهان. بنابر قضیهٔ ۱۰۵ ، $F[x]$ یک دامنهٔ صحیح است . $\varphi : F[x] - \{0\} \to \mathbf{N}$ را با $\varphi(f) = \deg f$ تعریف می‌کنیم . چون هر عنصر ناصفر F یک یکه است ، قضایای ۱۰۶ (چهار) و ۲۰۶ ایجاب می‌کنند که $F[x]$ یک دامنهٔ اقلیدسی باشد . بنابراین ، $F[x]$ یک دامنهٔ ایده‌آل اصلی و یک دامنهٔ یکتایی تجزیه است (قضیهٔ ۹۰۳) . بالاخره ، قضیهٔ ۱۰۶ (چهار) ایجاب می‌کند که هر یکهٔ f در $F[x]$ دارای درجهٔ صفر باشد ، که از آنجا f یک ثابت ناصفر می‌باشد . عکس مطلب واضح می‌باشد .

هرگاه F میدان باشد ، آنگاه $F[x_1, \ldots, x_n]$ یک دامنهٔ ایده‌آل اصلی نیست (تمرین ۱) ، ولی یک دامنهٔ یکتایی تجزیه هست (قضیهٔ ۱۴۰۶ در زیر) . پیش از اثبات این امر ، عوامل درجهٔ یک در حلقه‌های چندجمله‌ای را مورد بحث قرار می‌دهیم .

تعریف ۵۰۶ . فرض کنیم R زیرحلقه‌ای از حلقهٔ تعویضپذیر S باشد ، $c_1, c_2, \ldots, c_n \in S$ ،

و $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}} \in R[x_1, \ldots, x_n]$ یک‌چندجمله‌ای‌باشدبه‌طوری‌که $f(c_1, c_2, \ldots c_n) = 0$.

دراین‌صورت ،گوییم $(c_1, c_2, \ldots, c_n)$ یک **ریشه** یا **صفر** f (یایک **جواب** معادلهٔ چندجمله‌ای $f(x_1, \ldots, x_n) = 0$) است .[۱]

قضیهٔ ۶.۶ . فرض کنیم R یک حلقهٔ تعویضپذیریکدار بوده و $f \in R[x]$.در این صورت ، $c \in R$ یک ریشهٔ f است اگر و فقط اگر $x - c$ ، f را عاد کند .

طرح برهان . طبق‌نتیجهٔ ۳.۶ ،داریم $f(x) = q(x)(x - c) + f(c)$. هرگاه $x - c \mid f(x)$ ، آنگاه $f(c) = 0$ ؛ در نتیجه ، $h \in R[x]$ که $f(x) = q(x)(x - c) = h(x)(x - c)$ ؛ در نتیجه $(h(x) - q(x))(x - c) = f(c)$. چون R تعویضپذیراست ،نتیجهٔ ۶.۵ (به‌ازای $\varphi = 1_R$) ایجاب می‌کند که $f(c) = (h(c) - q(c))(c - c) = 0$. برای عکس قضیه تعویضپذیری لازم نیست ؛ از نتیجهٔ ۳.۶ استفاده کنید .

قضیهٔ ۷.۶ . هرگاه D یک دامنهٔ صحیح مشمول‌دامنهٔ صحیح E بوده و $f \in D[x]$ دارای درجهٔ n باشد ، آنگاه f حداکثر n ریشهٔ متمایز در E دارد .

طرح برهان . فرض کنیم $c_1, c_2, \ldots$ ریشه‌های**متمایزی**از f در E باشند. طبق قضیهٔ ۶.۶ ، $f(x) = q_1(x)(x - c_1)$ ، که از آنجا ، طبق نتیجهٔ ۶.۵ ، $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$. چون $c_1 \neq c_2$ و E دامنهٔ صحیح است ، $q_1(c_2) = 0$. بنابراین ، $x - c_2$ ، q_2 را عاد می‌کند و $f(x) = q_2(x)(x - c_2)(x - c_1)$.حال استدلال استقرایی نشان می‌دهد که هروقت $c_1, \ldots, c_m$ ریشه‌های‌متمایزی‌از f در E باشند .آنگاه $g_m = (x - c_1)(x - c_2)\cdots(x - c_m)$ f راعاد می‌کند . اما طبق قضیهٔ ۱۰۶ ، $\deg g_m = m$.بنابراین ،باز طبق قضیهٔ ۱۰۶ ، $m \leq n$.

---

۱ . اگر بین "ریشه‌های چپ" و "ریشه‌های راست" تمیز بگذاریم ، در تعریف تعویضپذیری لازم نیست (ریشه‌های راست وقتی رخ می‌دهد که f به صورت $f = \sum x_1^{k_{i1}} \cdots x_n^{k_{in}} a_i$ نوشته شود) .

تبصره. قضیهٔ ۷.۶ ممکن است بدون فرض تعویضپذیری درست نباشد. مثلاً "x^2+1" در حلقهٔ‌بخشی چهارتاهای حقیقی (شامل $\pm i$ ، $\pm j$ ، و $\pm k$) بی‌نهایت ریشهٔ متمایز دارد.

هرگاه D یک‌دامنهٔ یکتایی تجزیه با میدان خارج‌قسمتی F بوده و $f \in D[x]$ ، آنگاه ریشه‌های f در F ممکن است از طریق حکم زیر به دست آیند.

حکم ۸.۶. *فرض کنیم D یک دامنهٔ یکتایی تجزیه با میدان خارج‌قسمتی F بوده و* $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. *هرگاه* $u = c/d \in F$ ، *که در آن c و d نسبت به هم اولند ، و u ریشه‌ای از f باشد ، آنگاه c* ، a_0 *را عاد می‌کند و d* ، a_n *را عاد می‌کند.*

طرح برهان. $f(u) = 0$ ایجاب می‌کند که $a_0 d^n = c\left(\sum_{i=1}^{n} (-a_i)c^{i-1}d^{n-i}\right)$ و $-a_n c^n = \left(\sum_{i=0}^{n-1} c^i d^{n-i-1}\right)d$. درنتیجه ، هرگاه $(c,d) = 1_R$ ، آنگاه ، طبق تمرین ۱۰.۳ ، $c \mid a_0$ و $d \mid a_n$.

مثال. هرگاه $f = x^4 - 2x^3 - 7x^2 - (11/3)x - 4/3 \in \mathbf{Q}[x]$ ، آنگاه ریشه‌های f در $\mathbf{Q}$ همان ریشه‌های

$$3f = 3x^4 - 6x^3 - 21x^2 - 11x - 4 \in \mathbf{Z}[x]$$

در $\mathbf{Q}$ اند. بنابر حکم ۸.۶ ، تنها ریشه‌های گویای ممکن $3f$ عبارتند از ± 1 ، ± 2 ، ± 4 ، $\pm 1/3$ ، $\pm 2/3$ ، و $\pm 4/3$. جانشانی نشان می‌دهد که 4 تنها ریشهٔ گویاست.

فرض کنیم D دامنهٔ صحیح بوده و $f \in D[x]$. هرگاه $c \in D$ و c ریشه‌ای از f باشد ، آنگاه کاربرد مکرر قضیهٔ ۶.۶ همراه‌باقضیهٔ ۷.۶ نشان می‌دهد که بزرگترین عدد صحیح m $(0 \le m \le \deg f)$ وجود دارد به‌طوری‌که

$$f(x) = (x-c)^m g(x),$$

که در آن $g(x) \in R[x]$ و $x - c \nmid g(x)$ (یعنی ، $g(c) \neq 0$) . عدد صحیح m ***بستایی ریشهٔ*** c از f نام دارد. اگر c بستایی 1 داشته باشد ، گوییم c یک ***ریشهٔ ساده*** است. اگر c

بستایی $m > 1$ داشته باشد، c را یک **ریشهٔ چندگانه** نامیم. برای تعیین اینکه چه وقت یک چندجمله‌ای ریشه‌های چندگانه دارد، به لم زیر نیاز خواهیم داشت.

لم ۹۰۶. *فرض کنیم* D *یک دامنهٔ صحیح بوده و* $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. *همچنین،* $f' \in D[x]$ *چندجمله‌ای* $f' = \sum_{k=1}^{n} k a_k x^{k-1} = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}$ *باشد. در این صورت، به‌ازای هر* $f, g \in D[x]$ *و* $c \in D$،

(یک) $(cf)' = cf'$؛

(دو) $(f + g)' = f' + g'$؛

(سه) $(fg)' = f'g + fg'$؛

(چهار) $(g^n)' = n g^{n-1} g'$.

برهان. تمرین.

چندجمله‌ای f' *مشتق صوری* f نام دارد. واژهٔ "صوری" بر این تاکید دارد که تعریف f' مستلزم مفهوم حدود نیست.

بنابرتعریف ۳۰۳، چندجمله‌ای ناصفر $f \in R[x]$ ***تحویل‌ناپذیر*** است مشروط بر اینکه f یکه نبوده و در هر تجزیهٔ $f = gh$ یا g در $R[x]$ یکه باشد یا h.

قضیهٔ ۱۰۰۶. *فرض کنیم* D *یک دامنهٔ صحیح باشد که یک زیرحلقهٔ دامنهٔ صحیح* E *است. همچنین،* $f \in D[x]$ *و* $c \in E$.

(یک) c *یک ریشهٔ چندگانهٔ* f *است اگر و فقط اگر* $f(c) = 0$ *و* $f'(c) = 0$.

(دو) *هرگاه* D *میدان بوده و* f *نسبت به* f' *اول باشد، آنگاه* f *در* E *ریشهٔ چندگانه ندارد.*

(سه) *هرگاه* D *میدان،* f *در* $D[x]$ *تحویل‌ناپذیر، و* E *شامل ریشه‌ای از* f *باشد، آنگاه* f *ریشهٔ چندگانه‌ای در* E *ندارد اگر و فقط اگر* $f' \neq 0$.

برهان. (یک) $f(x) = (x - c)^m g(x)$، که در آن m بستایی f بوده $(m \geq 0)$ و

$g(c) \neq 0$. بنابر لم ۹۰۶ ، $f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x)$. هرگاه c یک ریشهٔ چندگانهٔ f باشد ، آنگاه $m > 1$ ، که از آنجا $f'(c) = 0$. به عکس، هرگاه $f(c) = 0$ ، آنگاه $m \geq 1$ (قضیهٔ ۶۰۶) . هرگاه $m = 1$ ، آنگاه $f'(x) = g(x) + (x-c)g'(x)$. درنتیجه ، هرگاه $f'(c) = 0$ ، آنگاه ، طبق نتیجهٔ ۶۰۵ ، $f'(c) = g(c) = 0$ ، که یک تناقض است . بنابراین ، $m > 1$.

(دو) بنابرنتیجهٔ ۴۰۶ و قضیهٔ ۱۱۰۳ ، به‌ازای $k,h \in D[x] \subset E[x]$ ی ، $kf + hf' = 1_D$. هرگاه c ریشهٔ چندگانه‌ای از f باشد ، آنگاه ، بنابر نتیجهٔ ۶۰۵ و قسمت (یک) ، $1_D = k(c)f(c) + h(c)f'(c) = 0$ ، که یک تناقض است . ازاینرو ، c یک ریشهٔ ساده می‌باشد .

(سه) هرگاه f تحویل‌ناپذیر بوده و $f' \neq 0$ ، آنگاه f و f' نسبت به هم اولند ، زیرا $\deg f' < \deg f$. بنابراین ، طبق قسمت (دو) ، f ریشهٔ چندگانه ندارد . به عکس ، فرض کنیم f در E ریشهٔ چندگانه‌نداشته و b ریشه‌ای از f در E باشد . هرگاه $f' = 0$ ، آنگاه ، طبق قسمت (یک) ، b یک ریشهٔ چندگانه‌است ، که تناقضی است . از اینرو ، $f' \neq 0$.

این امر بحث عوامل خطی چندجمله‌ایها را کامل می‌کند . حال مسئلهٔ کلیتر تعیین یکه‌ها و عناصر تحویل‌ناپذیر در حلقهٔ چندجمله‌ای $D[x]$ را درنظر می‌گیریم ، که در آن D یک دامنهٔ صحیح است . این مسئله عموما " مشکل است ، اما بعضی نکات به آسانی ثابت می‌شوند :

(یک) یکه‌ها در $D[x]$ دقیقا " چندجمله‌ایهای ثابت‌اند که در D یکه می‌باشند [ر . ک . برهان نتیجهٔ ۴۰۶] .

(دو) هرگاه $c \in D$ و c در D تحویل‌ناپذیر باشد ، آنگاه چندجمله‌ای ثابت c در $D[x]$ تحویل‌ناپذیر است [از قضیهٔ ۱۰۶ و قسمت (یک) استفاده کنید] .

(سه) هر چندجمله‌ای درجهٔ اول که ضریب پیشرو آن یک یکه در D باشد در $D[x]$ تحویل‌ناپذیر است . بخصوص ، هر چندجمله‌ای درجهٔ اول روی یک میدان تحویل‌ناپذیر است .

(چهار) فرض کنیم D یک زیرحلقه از دامنهٔ صحیح E بوده و $f \in D[x] \subset E[x]$. در این صورت ، همانطور که در مثالهای زیر دیده می‌شود ، f ممکن است در $E[x]$ تحویل‌ناپذیر باشد ولی در $D[x]$ نباشد و بالعکس .

چند مثال. بنابر قسمت (سه) فوق، $2x+2$ در $\mathbf{Q}[x]$ تحویل‌ناپذیر است. با اینحال، $2x+2=2(x+1)$ و، طبق قسمت (یک)، نه 2 در $\mathbf{Z}[x]$ یکه است نه $x+1$، که از آنجا $2x+2$ در $\mathbf{Z}[x]$ تحویل‌ناپذیر نیست. x^2+1 روی میدان حقیقی تحویل‌ناپذیر است، ولی روی میدان مختلط به صورت $(x+i)(x-i)$ تجزیه می‌شود. چون، طبق (یک) $x+i$ و $x-i$ در $\mathbf{C}[x]$ یکه نیستند، x^2+1 در $\mathbf{C}[x]$ تحویل‌ناپذیر نیست.

برای به دست آوردن معدود نتیجهٔ کلی موجود در این حیطه، بقیهٔ بحث را به چندجمله‌ایها روی دامنهٔ یکتایی تجزیهٔ D محدود می‌کنیم. مآلا" ثابت می‌کنیم که $D[x_1,\dots,x_n]$ نیزیک‌دامنهٔ یکتایی تجزیه است. برهان نیاز به مقدماتی دارد، که محکی برای تحویل‌ناپذیری در $D[x]$ نیز به دست می‌دهد.

فرض کنیم D یک دامنهٔ یکتایی تجزیه بوده و $f=\sum_{i=0}^{n} a_i x^i$ یک چندجمله‌ای ناصفر در $D[x]$ باشد. بزرگترین مقسوم‌علیه مشترک ضرایب $a_0,a_1,\dots,a_n$ را *احتوای* f نامیده و با $C(f)$ نشان می‌دهیم. به بیان دقیق، نماد $C(f)$ مبهم است، زیرا بزرگترین مقسوم‌علیه‌های مشترک منحصر به فرد نیستند. اما هر دو احتوای f لزوما" شریک هستند وهرشریک‌احتوای f نیزاحتوای f می‌باشد. هرگاه b و c در D شریک باشند، خواهیم نوشت $b\approx c$. $\approx$ یک رابطهٔ هم‌ارزی بر D است و چون D یک دامنهٔ صحیح است، بنابر قضیهٔ ۲۰۳ (چهار)، $b\approx c$ اگر و فقط اگر به‌ازای یکه‌ای مانند $u\in D$، $b=cu$. هرگاه $u\in D$ و $f\in D[x]$، آنگاه $C(uf)\approx uC(f)$ (تمرین ۴). هرگاه $f\in D[x]$ و $C(f)$ یک یکه در D باشد، آنگاه‌گوییم f *اولیه* است. واضح‌است‌که به‌ازای هرچندجمله‌ای $g\in D[x]$، $g=C(g)g_1$، که در آن g_1 اولیه است.

لم ۱۱۰۶ (گاوس[1]). *هرگاه D یک دامنهٔ یکتایی تجزیه بوده و $f,g\in D[x]$، آنگاه $C(fg)\approx C(f)C(g)$. بخصوص، حاصل‌ضرب چندجمله‌ایهای اولیه اولیه است.*

برهان. $f=C(f)f_1$ و $g=C(g)g_1$، که در آنها f_1,g_1 اولیه‌اند. درنتیجه، $C(fg)=C(C(f)f_1C(g)g_1)\approx C(f)C(g)C(f_1g_1)$. از اینرو، کافی است ثابت کنیم که f_1g_1 اولیه است (یعنی، $C(f_1g_1)$ یکه‌است). هرگاه $f_1=\sum_{i=0}^{n} a_i x^i$ و $g_1=\sum_{i=0}^{m} b_i x^i$، آنگاه

1. Gauss

$f_1g_1 = \sum_{k=0}^{m+n} c_k x^k$ ، که در آن $c_k = \sum_{i+j=k} a_i b_j$. هرگاه f_1g_1 اولیه نباشد ، آنگاه یک عنصر تحویل‌ناپذیر مانند p در R هست به‌طوری که به‌ازای هر k ، $p \mid c_k$. چون $C(f_1)$ یکه است ، $p \nmid C(f_1)$ ؛ درنتیجه ، کوچکترین عدد صحیح مانند s هست به‌طوری که

به‌ازای $i < s$ ، $p \mid a_i$ و $p \nmid a_s$.

به همین نحو ، کوچکترین عدد صحیح t وجود دارد به‌طوری‌که

به‌ازای $j < t$ ، $p \mid b_j$ و $p \nmid b_t$.

چون p ، $c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots + a_{s+t} b_0$ را عاد می‌کند، p باید $a_s b_t$ را عادکند . چون هر عنصر تحویل‌ناپذیر در D اول است ، $p \mid a_s$ یا $p \mid b_t$ و این یک تناقض است . بنابراین ، f_1g_1 اولیه می‌باشد .

لم ۱۲۰۶ . فرض کنیم D دامنهٔ یکتایی تجزیه با میدان خارج‌قسمتی F بوده و f و g چندجمله‌ایهای اولیه در D[x] باشند . در این صورت ، f و g در D[x] شریک هستند اگر و فقط اگر در F[x] شریک باشند .

برهان . هرگاه f و g در دامنهٔ صحیح $F[x]$ شریک باشند ، آنگاه به‌ازای یکه‌ای چون $u \in F[x]$ ، $f = gu$ (قضیهٔ ۲۰۳ (شش)) . بنابر نتیجهٔ ۴۰۶ ، $u \in F$ ، که از آنجا $u = b/c$ که $b, c \in D$ و $c \neq 0$. بنابراین ، $cf = bg$. چون $C(f)$ و $C(g)$ در D یکه‌اند ،

$$c = cC(f) = C(cf) = C(bg) = bC(g) = b.$$

بنابراین ، به‌ازای یکه‌ای چون $v \in D$ ، $b = cv$ و $cf = bg = vcg$ ، درنتیجه ، $f = vg$ (زیرا $c \neq 0$) ، که از آنجا f و g در $D[x]$ شریک‌اند . عکس لم بدیهی است .

لم ۱۳۰۶ . فرض کنیم D یک دامنهٔ یکتایی تجزیه با میدان خارج قسمتی F بوده و f یک چندجمله‌ای اولیه با درجهٔ مثبت در D[x] باشد . در این صورت ، f در D[x] تحویل‌ناپذیر است اگر و فقط اگر f در F[x] تحویل‌ناپذیر باشد .

طرح برهان . فرض کنیم f در $D[x]$ تحویل‌ناپذیربوده و $f = gh$ ، که در آن $g, h \in F[x]$ و $\deg g \geq 1$, $\deg h \geq 1$. دراین صورت ، $g = \sum_{i=0}^{n} (a_i/b_i) x^i$ و $h = \sum_{j=0}^{m} (c_j/d_j) x^j$ ، که در

آنها $a_i,b_i,c_i,d_i \in D$ و $b = b_0b_1\cdots b_n$. فرض کنیم $b_i \neq 0,\ d_i \neq 0$ و، به‌ازای هر i ،

$a = C(g_1)$ که $g_1 = ag_2$ ، آنگاه $g_1 = \sum_{i=0}^{n} a_ib_i^*x^i \in D[x]$ هرگاه $b_i^* = b_0b_1\cdots b_{i-1}b_{i+1}\cdots b_n$.

$g_2 \in D[x]$ ، و g_2 اولیه‌است . تحقیق کنید که $g = (1_D/b)g_1 = (a/b)g_2$ و $\deg g = \deg g_2$.

به همین نحو، $h = (c/d)h_2$ ، که در آن $c,d \in D$ ، $h_2 \in D[x]$ ، h_2 اولیه است، و $\deg h = \deg h_2$. درنتیجه، $f = gh = (a/b)(c/d)g_2h_2$ ، که از آنجا $bdf = acg_2h_2$. چون طبق فرض f و طبق لم ۱۱.۶ g_2h_2 اولیه است،

$$bd = bdC(f) = C(bdf) = C(acg_2h_2) = acC(g_2h_2) = ac.$$

همانند در برهان لم ۱۲.۶ ، شریک بودن bd و ac در D ایجاب می‌کند که f و g_2h_2 در $D[x]$ شریک باشند . درنتیجه، f در $D[x]$ تحویل‌ناپذیر نیست، که تناقض می‌باشد . بنابراین، f در $F[x]$ تحویل‌ناپذیر است .

به عکس، هرگاه f در $F[x]$ تحویل‌ناپذیر بوده و $f = gh$ که در آن $g,h \in D[x]$ ، آنگاه، طبق نتیجهٔ ۴.۶ ، یکی از g,h (مثلاً " g) ثابت است . لذا، $C(f) = gC(h)$. چون f اولیه است، g باید در D ، و درنتیجه در $D[x]$ ، یکه باشد . بنابراین، f در $D[x]$ تحویل‌ناپذیر می‌باشد .

قضیهٔ ۱۴.۶ . هرگاه D یک دامنهٔ یکتایی تجزیه باشد، آنگاه حلقهٔ چندجمله‌ای $D[x_1, \ldots, x_n]$ نیز چنین است .

تبصره. چون میدان F بداهتاً "یک‌دامنهٔ‌یکتایی تجزیه است، $F[x_1, \ldots, x_n]$ یک دامنهٔ یکتایی تجزیه می‌باشد .

طرح برهان ۱۴.۶ . فقط ثابت می‌کنیم $D[x]$ یک‌دامنهٔ یکتایی تجزیه است . چون طبق نتیجهٔ ۷.۵ $D[x_1, \ldots, x_n] = D[x_1, \ldots, x_{n-1}][x_n]$ ، برهان با یک استقرای معمولی تمام می‌شود . هرگاه $f \in D[x]$ درجهٔ مثبت داشته باشد، آنگاه $f = C(f)f_1$ که در آن f_1 یک چندجمله‌ای‌اولیه‌در $D[x]$ با درجهٔ‌مثبت است . چون D یک دامنهٔ یکتایی تجزیه است، یا $C(f)$ یکه است یا $C(f) = c_1c_2\cdots c_m$ که در آن هر c_i در D ، و درنتیجه در $D[x]$ ، تحویل‌ناپذیر است . فرض کنیم F میدان خارج قسمتی D باشد . چون $F[x]$ یک‌دامنهٔ

یکتایی تجزیه است (نتیجهٔ ۴۰۶) که شامل $D[x]$ می‌باشد، $f_1 = p_1^* p_2^* \cdots p_n^*$ که در آن هر p_i^* یک چندجمله‌ای تحویل‌ناپذیر در $F[x]$ است. برهان لم ۱۳۰۶ نشان می‌دهد که به‌ازای هر i ، $p_i^* = (a_i/b_i)p_i$ که در آن $a_i, b_i \in D$ ، $b_i \neq 0$ ، $a_i/b_i \in F$ ، $p_i \in D[x]$ ، و p_i اولیه‌است. واضح است‌که هر p_i در $F[x]$ تحویل‌ناپذیر است، لذا، طبق لم ۱۳۰۶، هر p_i در $D[x]$ تحویل‌ناپذیر می‌باشد. هرگاه $a = a_1 a_2 \cdots a_n$ و $b = b_1 b_2 \cdots b_n$ ، آنگاه $f_1 = (a/b)p_1 p_2 \cdots p_n$. درنتیجه، $bf_1 = ap_1 p_2 \cdots p_n$. چون f_1 و $p_1 p_2 \cdots p_n$ اولیه‌اند (لم ۱۱۰۶)، (مثل برهان لم ۱۲۰۶) نتیجه می‌شود که a و b در D شریک‌اند. لذا، $a/b = u$ ، که در آن u یک یکه در D است. بنابراین، اگر $C(f)$ یک غیریکه باشد، $f = C(f) f_1 = c_1 c_2 \cdots c_m (up_1) p_2 \cdots p_n$ که‌درآن‌هر c_i ، p_i ، و up_1 در $D[x]$ تحویل‌ناپذیر است. به همین نحو، اگر $C(f)$ یکه باشد، f حاصل‌ضرب عناصر تحویل‌ناپذیر در $D[x]$ است.

(یکتایی) فرض‌کنیم f یک چندجمله‌ای غیراولیه در $D[x]$ از درجهٔ مثبت باشد. تحقیق کنید که هر تجزیهٔ f به صورت حاصل‌ضربی از عناصر تحویل‌ناپذیر را می‌توان به شکل $f = c_1 c_2 \cdots c_m p_1 \cdots p_n$ نوشت‌که‌درآن c_i هادر D تحویل‌ناپذیرند، $C(f) = c_1 \cdots c_m$ ، و هر p_i در $D[x]$ تحویل‌ناپذیر (و درنتیجه، اولیه) و از درجهٔ مثبت است. فرض‌کنیم $f = d_1 \cdots d_r q_1 \cdots q_s$ ، که در آن هر d_i در D تحویل‌ناپذیر است، $C(f) = d_1 \cdots d_r$ ، وهر q_i در $D[x]$ اولیهٔ تحویل‌ناپذیر و از درجهٔ مثبت است. در این صورت، $c_1 c_2 \cdots c_n$ و $d_1 d_2 \cdots d_r$ در D شریک‌اند. یکتایی تجزیه در D ایجاب می‌کند که $n = r$ ، و (پس‌از اندیسگذاری مجدد) هر c_i یک شریک d_i می‌باشد. درنتیجه، $p_1 p_2 \cdots p_n$ و $q_1 q_2 \cdots q_s$ در $D[x]$ ، و لذا در $F[x]$ ، شریک هستند. چون بنابر لم ۱۳۰۶ هر p_i در $F[x]$ [q_i] تحویل‌ناپذیر است، یکتایی تجزیه در $F[x]$ (نتیجهٔ ۴۰۶) ایجاب می‌کند که $n = s$ و (پس‌از اندیسگذاری مجدد) هر p_i یک شریک q_i در $F[x]$ می‌باشد. بنابر لم ۱۲۰۶، هر p_i یک شریک q_i در $D[x]$ خواهد بود.

قضیهٔ ۱۵۰۶ (محک آیزنشتاین). *فرض‌کنیم D یک دامنهٔ یکتایی تجزیه با میدان خارج قسمتی F باشد. هرگاه* $f = \sum_{i=0}^{n} a_i x^i \in D[x]$ ، $\deg f \geq 1$ ، *و* p *یک عنصر تحویل ناپذیر D باشد به‌طوری‌که*

$$p \nmid a_n \text{ ؛ به‌ازای } p \mid a_i \text{ ، } i = 0, 1, \ldots, n-1 \text{ ؛ } p^2 \nmid a_0 \text{ ،}$$

آنگاه f در $F[x]$ تحویل‌ناپذیر است. هرگاه f اولیه باشد، آنگاه f در $D[x]$ تحویل ناپذیر است.

برهان. $f = C(f)f_1$، که در آن f_1 در $D[x]$ اولیه بوده و $C(f) \in D$؛ (بخصوص، اگر f اولیه باشد، $f_1 = f$). چون $C(f)$ در F یکه است (نتیجهٔ ۴.۶)، کافی است نشان دهیم که f_1 در $F[x]$ تحویل‌ناپذیر است. بنابر لم ۱۳.۶، فقط باید ثابت کنیم که f_1 در $D[x]$ تحویل‌ناپذیر است. فرض کنیم به عکس $f_1 = gh$، که در آن

$$g = b_r x^r + \cdots + b_0 \in D[x], \deg g = r \geq 1;$$

و

$$h = c_s x^s + \cdots + c_0 \in D[x], \deg h = s \geq 1.$$

اما p، $C(f)$ را عاد نمی‌کند (زیرا $p \nmid a_n$)؛ درنتیجه، ضرایب $f_1 = \sum_{i=0}^{n} a_i^* x^i$ درهمان شرایط بخشپذیری نسبت به p صدق می‌کنند که ضرایب f صدق می‌نمایند. چون p، $a_0^* = b_0 c_0$ را عاد می‌کند و هر عنصر تحویل‌ناپذیر در D اول است، یا $p \mid b_0$ یا $p \mid c_0$؛ مثلاً "، $p \mid b_0$. چون $p^2 \nmid a_0^*$، c_0 بر p بخشپذیر **نیست**. اما بعضی از ضرایب b_k از g بر p بخشپذیر نیستند (در غیر این صورت، p هر ضریب $gh = f_1$ را عاد می‌کرد که یک تناقض بود). فرض کنیم k کوچکترین عدد صحیحی باشد که

$$p \mid b_i, \quad i < k \quad \text{به‌ازای} \quad p \nmid b_k.$$

در این صورت، $1 \leq k \leq r < n$. چون $a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$ و $p \mid a_k^*$، p باید $b_k c_0$ را عادکند، که از آنجا p، b_k یا c_0 را عاد می‌کند. چون این تناقض است، f_1 باید در $D[x]$ تحویل‌ناپذیر باشد.

مثال. هرگاه $f = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbf{Z}[x]$، آنگاه محک آیزنشتاین به‌ازای $p = 3$ نشان می‌دهد که f در هر دوی $\mathbf{Q}[x]$ و $\mathbf{Z}[x]$ تحویل‌ناپذیر است.

مثال. فرض کنیم $f = y^3 + x^2y^2 + x^3y + x \in R[x,y]$ که در آن R یک‌دامنهٔ یکتایی‌تجزیه است. دراین صورت، x در $R[x]$ تحویل‌ناپذیر است و f به عنوان عنصری از $(R[x])[y]$ اولیه است. بنابراین، طبق قضیهٔ ۱۴.۶ و محک آیزنشتاین (با $p = x$ و $D = R[x]$)،

f در $R[x][y] = R[x,y]$ تحویل‌ناپذیر می‌باشد.

برای کاربرد دیگری از محک آیزنشتاین، ر.ک. تمرین ۱۰. روش طولانی دیگری (منسوب به‌کرونکر[1]) برای یافتن تمام عوامل تحویل‌ناپذیر یک چندجمله‌ای روی دامنهٔ یکتایی تجزیه‌ای که مثل $\mathbf{Z}$ فقط تعدادی متناهی یکه دارد، موجود است (تمرین ۱۳). امثله و تکنیکهای دیگر در تمرینهای ۶ تا ۹ خواهند آمد.

تمرینات

۱. (آ) هرگاه D یک دامنهٔ صحیح بوده و c عنصر تحویل‌ناپذیری در D باشد، آنگاه $D[x]$ یک دامنهٔ ایده‌آل اصلی نیست. [**راهنمایی.** ایده‌آل (x,c) تولید شده به وسیلهٔ x و c را درنظر بگیرید.]

(ب) $\mathbf{Z}[x]$ یک دامنهٔ ایده‌آل اصلی نیست.

(پ) هرگاه F میدان بوده و $n \geq 2$، آنگاه $F[x_1, \ldots, x_n]$ یک دامنهٔ ایده‌آل اصلی نیست. [**راهنمایی.** نشان‌دهیدکه x_1 در $F[x_1, \ldots, x_{n-1}]$ تحویل‌ناپذیر است.]

۲. هرگاه F میدان بوده و $f,g \in F[x]$ با $\deg g \geq 1$، آنگاه چندجمله‌ایهای منحصر به فرد $f_0,f_1, \ldots, f_r \in F[x]$ وجود دارند به‌طوری‌که به‌ازای هر i، $\deg f_i < \deg g$ و

$$f = f_0 + f_1 g + f_2 g^2 + \cdots + f_r g^r.$$

۳. فرض کنید f یک چندجمله‌ای از درجهٔ مثبت روی دامنهٔ صحیح D باشد.

(آ) هرگاه $\operatorname{char} D = 0$، آنگاه $f' \neq 0$.

(ب) هرگاه $\operatorname{char} D = p \neq 0$، آنگاه $f' = 0$ اگر و فقط اگر f یک چندجمله‌ای از x^p باشد (یعنی، $f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{ip} x^{ip}$).

۴. هرگاه D یک دامنهٔ یکتایی تجزیه بوده، $a \in D$، و $f \in D[x]$، آنگاه $C(af)$ و $aC(f)$ در D شریکاند.

۵. فرض کنید R یک‌حلقهٔ تعویضپذیریکدار بوده و $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. در این‌صورت،

---

1. Kronecker

f یک یکه در $R[x]$ است اگر و فقط اگر a_0 یک یکه در R بوده و $a_1, \ldots, a_n$ عناصر پوچ‌توانی از R باشند (تمرین ۱۲۰۱).

۶. فرض کنید $p \in \mathbf{Z}$ اول باشد. همچنین، F میدان بوده و $c \in F$. در این صورت، $x^p - c$ در $F[x]$ تحویل‌ناپذیر است اگر و فقط اگر $x^p - c$ در F ریشه نداشته باشد.
[**راهنمایی.** دو حالت در نظر بگیرید: $\operatorname{char} F = p$ و $\operatorname{char} F \neq p$.]

۷. اگر $f = \sum a_i x^i \in \mathbf{Z}[x]$ و p اول باشد، فرض کنید $\bar{f} = \sum \bar{a}_i x^i \in Z_p[x]$، که در آن $\bar{a}$ نقش a تحت بروریختی کانونی $\mathbf{Z} \to Z_p$ است.

(آ) هرگاه f تکین بوده و $\bar{f}$ به‌ازای عدد اولی چون p در $Z_p[x]$ تحویل‌ناپذیر باشد، آنگاه f در $\mathbf{Z}[x]$ تحویل‌ناپذیر است.

(ب) با مثال نشان دهید که (آ) ممکن است در صورت تکین نبودن f درست نباشد.

(پ) قسمت (آ) را به چندجمله‌ایها روی دامنهٔ یکتایی تجزیه تعمیم دهید.

۸. (آ) فرض کنید $c \in F$، که در آن F میدان مشخص p (p اول) است. در این صورت، $x^p - x - c$ در $F[x]$ تحویل‌ناپذیر است اگر و فقط اگر $x^p - x - c$ ریشه‌ای در F نداشته باشد. (ب) اگر $\operatorname{char} F = 0$، قسمت (آ) درست نیست.

۹. فرض کنید $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$ دارای درجهٔ n باشد. همچنین، به‌ازای k ای $(0 < k < n)$ و p ی اولی، $p \nmid a_n$؛ به‌ازای هر $0 \leq i \leq k-1$، $p \mid a_i$؛ و $p \nmid a_k$؛ و $p^2 \nmid a_0$. نشان دهید f عاملی چون g از درجهٔ حداقل k دارد که در $\mathbf{Z}[x]$ تحویل‌ناپذیر است.

۱۰. (آ) فرض کنید D دامنهٔ صحیح بوده و $c \in D$. همچنین، $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ و $f(x-c) = \sum_{i=0}^{n} a_i (x-c)^i \in D[x]$. در این صورت، $f(x)$ در $D[x]$ تحویل‌ناپذیر است اگر و فقط اگر $f(x-c)$ تحویل‌ناپذیر باشد.

(ب) به‌ازای هر p اول، **چندجمله‌ای دایره بر** $f = x^{p-1} + x^{p-2} + \cdots + x + 1$ در $\mathbf{Z}[x]$ تحویل‌ناپذیر است. [**راهنمایی.** توجه کنید که $f = (x^p - 1)/(x - 1)$، که از آنجا $f(x+1) = ((x+1)^p - 1)/x$. با استفاده از قضیهٔ دوجمله‌ای ۶۰۱ و

محک آیزنشتاین، نشان دهید که $f(x+1)$ در $\mathbf{Z}[x]$ تحویل‌ناپذیر است.]

۱۱. هرگاه $c_0, c_1, \ldots, c_n$ عناصر متمایزی از دامنهٔ صحیح D بوده و $d_0, \ldots, d_n$ عنصرهایی از D باشند، آنگاه حداکثر یک چندجمله‌ای مانند f از درجهٔ $n+1$ در $D[x]$ هست به‌طوری‌که به‌ازای $i = 0,1,\ldots,n$ ، $f(c_i) = d_i$. [برای وجود f ، ر.ک. تمرین ۱۲.]

۱۲. **فرمول درونیابی لاگرانژ.** هرگاه F میدان، $a_0, a_1, \ldots, a_n$ عناصر متمایزی از F ، و $c_0, c_1, \ldots, c_n$ عناصر دلخواهی از F باشند، آنگاه

$$f(x) = \sum_{i=0}^{n} \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} c_i$$

چندجمله‌ای منحصر به فردی در $F[x]$ است به‌طوری که به‌ازای هر i ، $f(a_i) = c_i$ [ر.ک. تمرین ۱۱].

۱۳. فرض کنید D یک دامنهٔ یکتایی تجزیه با تعدادی متناهی یکه و میدان خارج‌قسمتی F باشد. هرگاه $f \in D[x]$ دارای درجهٔ n بوده و $c_0, c_1, \ldots, c_n$ ، $n+1$ عنصر متمایز از D باشند، آنگاه f برطبق تمرین ۱۱ کاملا" با $f(c_0), f(c_1), \ldots, f(c_n)$ معین می‌شود. **روش کرونکر** برای یافتن تمام عوامل تحویل‌ناپذیر f در $D[x]$ ذیلا" ذکر می‌شود.

(آ) کافی است فقط عوامل g از درجهٔ حداکثر $n/2$ یافت شود.

(ب) هرگاه g عاملی از f باشد، آنگاه، به‌ازای هر $c \in D$ ، $g(c)$ عاملی از $f(c)$ است.

(پ) فرض کنید m بزرگترین عدد صحیح نابیشتر از $n/2$ بوده و عناصر متمایز $c_0, c_1, \ldots, c_m \in D$ را اختیار کنید. $d_0, d_1, \ldots, d_m \in D$ را طوری بگیرید که به‌ازای هر i ، d_i عاملی از $f(c_i)$ باشد. با استفاده از تمرین ۱۲، چندجمله‌ای $g \in F[x]$ را طوری بسازید که به‌ازای هر i ، $g(c_i) = d_i$؛ بنابر تمرین ۱۱، این چندجمله‌ای منحصر به فرد است.

(ت) تحقیق کنید که چندجمله‌ای g قسمت (پ) عاملی از f در $F[x]$ هست یا نه. اگر نیست، $d_0, \ldots, d_m$ را مجددا" انتخاب کرده و قسمت (پ) را تکرار کنید. (چون D یک دامنهٔ یکتایی تجزیه بوده و فقط تعدادی متناهی یکه دارد، فقط تعدادی متناهی انتخاب برای $d_0, \ldots, d_m$ وجوددارد.) هرگاه g عاملی از f باشد،

مثلا " $f = gh$ ، آنگاه کل فرایند را به ازای g و h تکرار کنید .

(ث) پس از چند مرحله تمام عوامل (تحویل‌ناپذیر) f در $F[x]$ به دست می‌آیند . هرگاه $g \in F[x]$ چنین عاملی (از درجهٔ مثبت) باشد ، آنگاه $r \in D$ را طوری اختیار می‌کنیم که $rg \in D[x]$ (مثلا " ، فرض‌کنید r حاصل‌ضرب مخرجهای ضرایب g باشد) . در این صورت ، $r^{-1}(rg)$ ، و درنتیجه rg ، عاملی از f است . پس $rg = C(rg)g_1$ که در آن $g_1 \in D[x]$ در $F[x]$ اولیه و تحویل‌ناپذیر است . بنابر لم ۱۳۰۶ ، g_1 عامل تحویل‌ناپذیری از f در $D[x]$ است . با ادامهٔ این کار ، تمام عوامل تحویل ناپذیر غیرثابت f به دست می‌آیند ؛ سپس ثابتها به آسانی به دست می‌آیند .

۱۴ . فرض کنید R حلقهٔ تعویضپذیر یکداری بوده و $c,b \in R$ که c یک یکه است .

(آ) نشان دهید که انتساب $x \mapsto cx + b$ خودریختی منحصر به فردی از $R[x]$ را القا می‌کند که همانی R است . معکوس آن چیست ؟

(ب) هرگاه D یک دامنهٔ صحیح باشد ، آنگاه نشان دهید هر خودریختی $D[x]$ که بر D همانی باشد از نوع توصیف شده در (آ) است .

۱۵ . هرگاه F میدان باشد ، آنگاه x و y در دامنهٔ $F[x,y]$ از چندجمله‌ایها نسبت به هم اولند ، ولی $(x) + (y) \subsetneq (1_F) = F[x,y]$ [با قضیهٔ ۱۱۰۳ (یک) مقایسه‌نمایید] .

۱۶ . فرض کنید $f = a_n x^n + \cdots + a_0$ یک چندجمله‌ای روی میدان $\mathbf{R}$ اعداد حقیقی بوده و $\varphi = |a_n|x^n + \cdots + |a_0| \in \mathbf{R}[x]$.

(آ) هرگاه به‌ازای $i = 1, \ldots, n$ ، $|u_i| \leq d_i$ ، آنگاه $|f(u_1, \ldots, u_n)| \leq \varphi(d_1, \ldots, d_n)$.

[به یاد آورید که $|a| \leq a', |b| \leq b' \Rightarrow |ab| \leq a'b'$ و $|a + b| \leq |a| + |b|$.]

(ب) به فرض آنکه $a,c \in \mathbf{R}$ با $c > 0$ ، $M \in \mathbf{R}$ ی هست به‌طوری‌که به‌ازای هر $h \in \mathbf{R}$ که $|h| \leq c$ ، $|f(a + h) - f(a)| \leq M|h|$. [**راهنمایی** . از قسمت (آ) استفاده کنید .]

(پ) (قضیهٔ مقدار میانی) هرگاه $a < b$ و $f(a) < d < f(b)$ ، آنگاه $c \in \mathbf{R}$ ای وجود دارد به‌طوری‌که $a < c < b$ و $f(c) = d$. [**راهنمایی** . فرض کنید c کوچکترین کران بالایی $S = \{x \mid a < x < b \text{ و } f(x) \leq d\}$ باشد . از قسمت (ب) استفاده کنید .]

(ت) هرچندجمله‌ای g از درجهٔ فرد در $\mathbf{R}[x]$ ریشه‌ای حقیقی دارد .

[**راهنمایی** . به‌ازای $a,b \in \mathbf{R}$ مناسب ، $g(a) < 0$ و $g(b) > 0$ ؛ از قسمت (پ) استفاده کنید .]

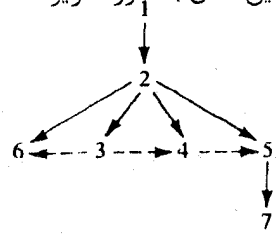
۴

مدولها

مدولهاروی یک حلقه تعمیمی ازگروههای‌آبلی‌اند (که مدولهایی روی $\mathbf{Z}$ می‌باشند) .اینها در مطالعهٔ‌جبرپیشرفته ازاساس می‌باشند . قسمت اعظم بخش ۱ به انتقال مفاهیم و نتایج نظریهٔ‌گروهها به مدولها اختصاص دارد . با آنکه رده‌بندی (با تقریب یکریختی) مدولها روی یک حلقهٔ دلخواه نسبتا" سخت است ، ولی برای مدولهای آزاد روی یک حلقه (بخش ۲) و مدولهای با تولید متناهی روی یک دامنهٔ ایده‌آل اصلی (بخش ۶) نتایجی اساسا "کامل دردست می‌باشد . مدولهای آزاد ، که فضاهای برداری روی یک حلقهٔ بخشی حالات خاصی از آنهایند ، کاربردهای گسترده‌ای داشته و در بخش ۲ به‌طور جامع بررسی می‌شوند . مدولهای تصویری (تعمیمی از مدولهای آزاد) در بخش ۳ مطرح می‌شوند ؛ این مطالب فقط در بخش VIII ۶۰ و فصل نه لازم خواهند بود .

به‌استثنای بخشهای۲ و ۶ ، توجه ما به ساختارهای خارجی مدولهاست تا ساختار داخلی‌آنها .مباحثی که مورد توجه خاصند عبارتند از جنبه‌های رسته‌ای نظریهٔ مدولها : دنباله‌های کامل (بخش ۱) و همریختیهای مدولها (بخش ۴) . به علاوه ، ساختهای مختلفی‌در رابطه با مدولها از قبیل ضرب تانسوری مطالعه خواهد شد (بخش ۵) . جبرها روی حلقهٔ تعویضپذیر یکدار K در بخش ۷ معرفی خواهند شد .

ارتباط تقریبی بخشهای این فصل به صورت زیر است :



سهم شکستهٔ $B \dashrightarrow A$ مبین آن است که گاهی در بخش B از نتایج بخش A استفاده می‌شود، ولی B اساساً از بخش A مستقل است.

۱ مدولها، همریختیها، و دنباله‌های کامل

مدولها روی یک حلقه تعمیمی از گروههای آبلی‌اند (که مدولهایی روی $\mathbf{Z}$ می‌باشند). درنتیجه، قسمت اول این بخش عمدتاً به انتقال مفاهیم و نتایج مختلف نظریهٔ گروهها به‌مدولها می‌پردازد. باقی این بخش نکات اساسی دنباله‌های کامل را دربرخواهد داشت.

تعریف ۱.۱. فرض کنیم R یک حلقه باشد. یک **R-مدول** (چپ) گروهی آبلی و جمعی مانند A است همراه با تابعی مانند $R \times A \to A$ (نقش (r,a) با ra نموده می‌شود) به طوری‌که به‌ازای هر $r,s \in R$ و $a,b \in A$،

(یک) $r(a+b) = ra + rb$؛

(دو) $(r+s)a = ra + sa$؛

(سه) $r(sa) = (rs)a$.

هرگاه R دارای واحد 1_R بوده و

(چهار) به‌ازای هر $a \in A$، $1_R a = a$،

آنگاه گوییم A یک R ــ **مدول یکانی** است. هرگاه R یک حلقهٔ بخشی باشد، آنگاه یک R ــ مدول یکانی یک ***فضای برداری*** (چپ) نام دارد.

یک R ــ مدول راست (یکانی) به همین نحو با تابعی چون $A \times R \to A$ تعریف می‌شود که با $(a,r) \mapsto ar$ نموده‌شده‌ودرمشابه‌های واضح (یک) تا (چهار) صدق می‌کند. از حالا به بعد (مگر به صورتی‌دیگر تصریح شود)، "R ــ مدول" یعنی "R ــ مدول‌چپ" و فرض این‌است‌که تمام قضایای مربوط به R ــ مدولها، ***نعل به نعل***، برای R ــ مدولهای راست برقرارند.

گروه A ممکن است ساختارهای R-مدول بسیاری (چپ و راست) داشته باشد. اگر R تعویضپذیر باشد، به‌آسانی تحقیق می‌شود که به هر R ــ مدول چپ A می‌توان با تعریف $ar = ra$ به‌ازای $r \in R, a \in A$ ساختار R ــ مدول راست داد (تعویضپذیری برای قسمت (سه) لازم است؛ برای تعمیمی از این ایده به حلقه‌های دلخواه، ر.ک. تمرین ۱۶).

فرض می‌کنیم هر مدول A روی حلقهٔ **تعویضپذیر** R هم مدول چپ است هم مدول راست که در آن به‌ازای هر $r \in R, a \in A$ ، $ar = ra$ مگر آنکه خلافش تصریح شود .

هرگاه A مدولی با عنصر همانی جمعی 0_A روی حلقهٔ R با همانی جمعی 0_R باشد ، آنگاه به آسانی معلوم می‌شود که به‌ازای هر $r \in R, a \in A$ ،

$$r0_A = 0_A \quad \text{و} \quad 0_R a = 0_A .$$

در آینده $0_A, 0_R, 0 \in \mathbf{Z}$ و مدول بدیهی $\{0\}$ با 0 نموده خواهد شد .

همچنین ، به آسانی معلوم می‌شود که به‌ازای هر $r \in R$ ، $n \in \mathbf{Z}$ ، و $a \in A$ ،

$$(-r)a = -(ra) = r(-a) \quad \text{و} \quad n(ra) = r(na) ,$$

که در آن na همان معنی عادی خود در گروهها را دارد (تعریف I ۸.۱۰ ، نماد جمعی) .

مثال . هر گروه آبلی جمعی G یک $\mathbf{Z}$ ــ مدول یکانی است ، که در آن na $(n \in \mathbf{Z}, a \in G)$ با تعریف I ۸.۱۰ داده می‌شود .

مثال . هرگاه S یک حلقه و R یک زیرحلقه باشد ، آنگاه S یک R ــ مدول است (ولی عکس آن برقرار نیست !) که در آن ra $(r \in R, a \in S)$ ضرب در S است . بخصوص ، حلقه‌های $R[x_1, \ldots, x_m]$ و $R[[x]]$ ، R ــ مدول می‌باشند .

چند مثال . هرگاه I یک ایده‌آل **چپ** حلقهٔ R باشد آنگاه I یک R ــ مدول **چپ** است ، که در آن ra $(r \in R, a \in I)$ حاصلضرب معمولی در R می‌باشد . بخصوص ، 0 و R ، R ــ مدول می‌باشند . به علاوه ، چون I یک زیرگروه جمعی R است ، R/I یک گروه (آبلی) می‌باشد . R/I یک R ــ مدول است که در آن $r(r_1 + I) = rr_1 + I$. اما R/I لزوماً حلقه نیست ، مگر آنکه I یک ایده‌آل دوطرفه باشد .

مثال . فرض کنیم R و S حلقه بوده و $\varphi : R \to S$ یک همریختی حلقه‌ها باشد . در این صورت ، هر S ــ مدول A را می‌توان با تعریف کردن rx $(x \in A)$ مساوی $\varphi(r)x$ به یک R ــ مدول بدل کرد . گوییم ساختار R ــ مدول A به وسیلهٔ **برگشت در امتداد** φ داده شده است .

مثال. فرض کنیم A گروهی آبلی و $\mathrm{End}\ A$ حلقهٔ درونریختیهای آن باشد (ر.ک. ص ۱۸۱). در این صورت، A یک $(\mathrm{End}\ A)$ ــ مدول یکانی است، که در آن fa مساوی $f(a)$ (به‌ازای $f \in \mathrm{End}\ A$) تعریف می‌شود.

مثال. اگر R حلقه‌باشد، هرگروه آبلی را می‌توان با تعریف $ra = 0$، به‌ازای هر $r \in R$ و $a \in A$، به یک R ــ مدول با **ساختار مدولی بدیهی** تبدیل کرد.

تعریف ۲۰۱. فرض‌کنیم A و B مدولهایی روی حلقهٔ R باشند. تابع $f : A \to B$ یک **همریختی R ــ مدولها**ست مشروط بر اینکه به‌ازای هر $a,c \in A$ و $r \in R$،

$$f(a + c) = f(a) + f(c) \quad \text{و} \quad f(ra) = rf(a).$$

هرگاه R یک حلقهٔ بخشی باشد، آنگاه هر همریختی R ــ مدولها یک **تبدیل خطی** نام دارد.

وقتی از قراین معلوم باشد، همریختیهای R ــ مدولها فقط همریختی نامیده می‌شوند. توجه کنید که همریختی $f : A \to B$ از R ــ مدولها لزوماً همریختی گروههای آبلی‌جمعی می‌باشد. درنتیجه، همان اصطلاح به کار می‌رود: f یک **تکریختی R ــ مدولها** [یا **بروریختی** یا **یکریختی**] است اگر به‌عنوان نگاشتی از مجموعه‌ها انژکتیو [یا سورژکتیو یا بیژکتیو] باشد. **هستهٔ** f هستهٔ آن به عنوان یک همریختی گروههای آبلی است؛ یعنی، $\mathrm{Ker}\ f = \{a \in A \mid f(a) = 0\}$، به همین نحو، **نقش** f مجموعهٔ زیراست:

$$\mathrm{Im}\ f = \{b \in B \mid b = f(a) \text{ ای، } a \in A \text{ به‌ازای}\}$$

بالاخره، قضیهٔ ۳۰۲۰ I ایجاب می‌کند که

(یک) f یک تکریختی R ــ مدولهاست اگر و فقط اگر $\mathrm{Ker}\ f = 0$؛

(دو) $f : A \to B$ یک یکریختی R ــ مدولهاست اگر و فقط اگر یک همریختی R ــ مدولها مانند $g : B \to A$ موجود باشد به‌طوری که $gf = 1_A$ و $fg = 1_B$.

چند مثال. به‌ازای هر مدول، نگاشت صفر $0 : A \to B$ داده شده با $(a \in A)\ a \mapsto 0$ یک همریختی مدولهاست. هر همریختی گروههای آبلی یک همریختی $\mathbf{Z}$ ــ مدولهاست. اگر R حلقه باشد، نگاشت $R[x] \to R[x]$ داده شده با $f \mapsto xf$ (مثلاً، $(x^2 + 1) \mapsto x(x^2 + 1)$) یک

یک همریختی R ــ مدولهاست، ولی یک همریختی حلقه‌ها نیست.

تبصره. بـه‌ازای حلقـهٔ R، واضح است که ردهٔ تمام R ــ مدولها [یا R ــ مدولهای یکانی] و همریختیهای R ــ مدولها یک رسته (ملموس) تشکیل می‌دهند. درواقع، می‌توان برو ریختیها و تکریختیها را صرفا "با اصطلاحات رسته‌ای (فقط اشیاء و ریختها ــ نه عناصر) تعریف کرد"؛ ر.ک. تمرین ۲.

تعریف ۳.۱. فرض کنیم R یک‌حلقه، A یک R ــ مدول، و B زیرمجموعه‌ای ناتهی از A باشد. B یک **زیرمدول** A است مشروط بر اینکه B یک زیرگروه جمعی A بوده و، به‌ازای هـر $r\in R, b\in B$، $rb\in B$. هر زیرمدول یک فضای برداری روی یک حلقهٔ بخشی یک **زیرفضا** نام دارد.

توجه‌کنیدکه هر زیرمدول خود مدول است. همچنین، هر زیرمدول یک مدول یکانی روی یک حلقهٔ یکدار لزوما" یکانی است.

چند مثال. هرگاه R یک‌حلقه بوده و $f: A\to B$ یک همریختی R ــ مدولها باشد، آنگاه $\operatorname{Ker} f$ یک زیرمدول A است و $\operatorname{Im} f$ یک زیرمدول B می‌باشد. هرگاه C زیرمدولی از B باشد، آنگاه $f^{-1}(C)=\{a\in A \mid f(a)\in C\}$ زیرمدولی از A می‌باشد.

مثال. فرض کنیم I یک ایده‌آل‌چپ حلقهٔ R، A یک R ــ مدول، و S زیرمجموعه‌ای ناتهی از A باشد. در این صورت،

$$IS=\left\{\sum_{i=1}^{n} r_i a_i \mid r_i\in I; a_i\in S; n\in \mathbf{N}^*\right\}$$

زیرمدولی از A می‌باشد (تمرین ۳). به‌همین نحو، هرگاه $a\in A$، آنگاه $Ia=\{ra \mid r\in I\}$ یک زیرمدول A است.

مثال. هرگاه $\{B_i \mid i\in I\}$ خانواده‌ای از زیرمدولهای مدول A باشد، آنگاه به‌آسانی معلوم می‌شود که $\bigcap_{i\in I} B_i$ زیرمدولی از A است.

تعریف ۴.۱ . هرگاه X زیرمجموعه‌ای از مدول A روی حلقهٔ R باشد، آنگاه اشتراک تمام زیرمدولهای A شامل X **زیرمدول تولید شده به وسیلهٔ** X (یا **پیموده شده به‌وسیلهٔ** X) نام دارد.

اگر X متناهی بوده و X مدول B را تولید کند، گوییم B با **تولید عنصر متناهی** است. هرگاه $X = \varnothing$، آنگاه X بوضوح مدول صفر است. هرگاه X فقط از یک عنصر تشکیل شده باشد، یعنی $X = \{a\}$، آنگاه زیرمدول تولید شده به وسیلهٔ X ***(زیر)مدول دوری*** تولید شده به وسیلهٔ a نام دارد. بالاخره، هرگاه $\{B_i \mid i \in I\}$ خانواده‌ای از زیرمدولهای A باشد، آنگاه زیرمدول تولید شده به وسیلهٔ $X = \bigcup_{i \in I} B_i$ **مجموع** مدولهای B_i نامیده می‌شود. اگر مجموعهٔ اندیسگذار I متناهی باشد، مجموع B_n ,...,B_1 با $B_1 + B_2 + \cdots + B_n$ نموده می‌شود.

قضیهٔ ۵.۱ . *فرض کنیم R یک حلقه، A یک R ـ مدول، X زیرمجموعه‌ای از A، $\{B_i \mid i \in I\}$ خانواده‌ای از زیرمدولهای A باشد، و $a \in A$. همچنین، $Ra = \{ra \mid r \in R\}$.*

(یک) Ra زیرمدولی از A است و نگاشت $R \to Ra$ داده شده با $r \mapsto ra$ یک بروریختی R ـ مدولهاست.

(دو) زیرمدول دوری C تولید شده به‌وسیلهٔ a عبارت است از $\{ra + na \mid r \in R; n \in \mathbf{Z}\}$. هرگاه R یکدار بوده و C یکانی باشد، آنگاه $C = Ra$.

(سه) زیرمدول D تولید شده به وسیلهٔ X عبارت است از

$$\left\{\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j \mid s,t \in \mathbf{N}^*;\ a_i, b_j \in X;\ r_i \in R;\ n_j \in \mathbf{Z}\right\}.$$

هرگاه R یکدار بوده و A یکانی باشد، آنگاه

$$D = RX = \left\{\sum_{i=1}^{s} r_i a_i \mid s \in \mathbf{N}^*;\ a_i \in X;\ r_i \in R\right\}.$$

(چهار) مجموع خانوادهٔ $\{B_i \mid i \in I\}$ از تمام مجموعه‌های متناهی $b_{i_1} + \cdots + b_{i_n}$ که $b_{i_k} \in B_{i_k}$ تشکیل شده است.

برهان . تمرین؛ توجه کنید که هرگاه R دارای واحد 1_R بوده و A یکانی باشد، آنگاه، به‌ازای هر $n \in \mathbf{Z}$، $n1_R \in R$، و به‌ازای هر $a \in A$، $na = (n1_R)a$.

قضیهٔ ۶۰۱ . *فرض کنیم B زیرمدول مدول A روی حلقهٔ R باشد . در این صورت ،گروه خارج‌قسمتی A/B یک R ــ مدول است که عمل R بر A/B به صورت زیر داده می‌شود :*

$$r(a + B) = ra + B \quad ، \quad r \in R, a \in A \text{ به‌ازای هر}$$

نگاشت $\pi : A \to A/B$ داده شده با $a \mapsto a + B$ یک برووریختی R ــ مدولها با هستهٔ B است .

نگاشت π برووریختی کانونی (یا تصویر) نام دارد.

طرح برهان ۶۰۱ . چون A یک گروه آبلی جمعی است ، B یک زیرگروه نرمال است ، و A/B یک گروه آبلی تعریف شده می‌باشد . هرگاه $a + B = a' + B$ ، آنگاه $a - a' \in B$. چون B یک زیرمدول است ، به‌ازای هر $r \in R$ ، $ra - ra' = r(a - a') \in B$. لذا ، طبق نتیجهٔ I ۳۰۴۰ ، $ra + B = ra' + B$ و عمل R بر A/B تعریف شده است . حال بقیهٔ برهان آسان است .

در پرتو نتایج پیش،برقراری قضایای مختلف یکریختی گروهها (قضایای I ۶۰۵۰ تا I ۱۲۰۵۰) ، *نعل به نعل* برای مدولها تعجب‌آور نیست . کافی است هر مرحلهٔ برهان را تحقیق کرده‌ببینیم که‌هرزیرگروه یا همریختی یک زیرمدول یا همریختی مدولها می‌باشد . برای راحتی ، نتایج را در اینجا ذکر می‌کنیم .

قضیهٔ ۷۰۱ . *هرگاه R یک حلقه ، $f : A \to B$ یک همریختی R ــ مدولها ، و C یک زیرمدول $Ker\, f$ باشد ، آنگاه یک همریختی R ــ مدولهای منحصر به فرد مانند $\bar{f} : A/C \to B$ وجود دارد به‌طوری‌که به‌ازای هر $a \in A$ ، $\bar{f}(a + C) = f(a)$ ، $Im\, \bar{f} = Im\, f$. $\bar{f}$ یک یکریختی R ــ مدولهاست اگروفقط اگر f یک‌برووریختی R ــ مدولها بوده و $C = Ker\, f$. بخصوص ، $A/Ker\, f \cong Im\, f$.*

برهان . ر.ک. قضیهٔ I ۶۰۵۰ و نتیجهٔ I ۷۰۵۰ .

نتیجهٔ ۸۰۱ . *هرگاه R یک حلقه ، A' یک زیرمدول R ــ مدول A ، B' یک زیرمدول R ــ مدول B ، و $f : A \to B$ یک همریختی R ــ مدولها باشد به‌طوری‌که $f(A') \subset B'$ ،*

آنگاه f *یک همریختی* R *ـ مدولها مانند* $\bar{f}: A/A' \to B/B'$ *القا می‌کند که با* $a + A' \mapsto f(a) + B'$ *داده می‌شود.* $\bar{f}$ *یک یکریختی* R *ـ مدولهاست اگر و فقط اگر* $Im\, f + B' = B$ *و* $f^{-1}(B') \subset A'$. *بخصوص، هرگاه* f *یک بروریختی باشد به‌طوری‌که* $f(A') = B'$ *و* $Ker\, f \subset A'$، *آنگاه* f *یک یکریختی* R *ـ مدولهاست.*

برهان. ر.ک. نتیجهٔ I ۸۰۵۰.

قضیهٔ ۹۰۱. *فرض کنیم* B *و* C *زیرمدولهایی از مدول* A *روی حلقهٔ* R *باشد.*
(یک) یک یکریختی R *ـ مدولها مانند* $B/(B \cap C) \cong (B + C)/C$ *وجود دارد؛*
(دو) هرگاه $C \subset B$، *آنگاه* B/C *یک‌زیرمدول* A/C *است، و یک یکریختی* R *ـ مدولها مانند* $(A/C)/(B/C) \cong A/B$ *وجود دارد.*

برهان. ر.ک. نتایج I ۹۰۵۰ و I ۱۰۰۵۰.

قضیهٔ ۱۰۰۱. *هرگاه* R *یک حلقه بوده و* B *زیرمدولی از* R *ـ مدول* A *باشد، آنگاه تناظر یک‌به‌یکی بین مجموعهٔ تمام زیرمدولهای* A *شامل* B *و مجموعهٔ تمام زیرمدولهای* A/B *وجود دارد که با* $C \mapsto C/B$ *داده می‌شود. از اینرو، هر زیرمدول* A/B *به شکل* C/B *است، که در آن* C *زیرمدولی از* A *شامل* B *می‌باشد.*

برهان. ر.ک. قضیهٔ I ۱۱۰۵۰ و نتیجهٔ I ۱۲۰۵۰.

حال نشان می‌دهیم که حاصلضربها و هم حاصلضربها همواره در رستهٔ R ـ مدولها وجود دارند.

قضیهٔ ۱۱۰۱. *فرض کنیم* R *حلقه،* $\{A_i \mid i \in I\}$ *خانواده‌ای ناتهی از* R *ـ مدولها،* $\prod_{i \in I} A_i$ *حاصلضرب مستقیم گروههای آبلی* A_i، *و* $\sum_{i \in I} A_i$ *مجموع مستقیم گروههای آبلی* A_i *باشد.*

(یک) $\prod_{i\in I} A_i$ یک R ــ مدول با عمل R است که با $r\{a_i\} = \{ra_i\}$ داده می‌شود.

(دو) $\sum_{i\in I} A_i$ یک‌زیرمدول $\prod_{i\in I} A_i$ است.

(سه) به‌ازای هر $k \in I$، تصویرکانونی $\pi_k : \prod A_i \to A_k$ (قضیهٔ I ۱۰۸۰) یک بروریختی R ــ مدولهاست.

(چهار) به‌ازای هر $k \in I$، انژکسیون کانونی $\iota_k : A_k \to \sum A_i$ (قضیهٔ I ۴۰۸۰) یک تکریختی R ــ مدولهاست.

برهان. تمرین.

$\prod_{i\in I} A_i$ حاصل‌ضرب مستقیم (خارجی) خانوادهٔ $\{A_i \mid i \in I\}$ از R ــ مدولهاو $\sum_{i\in I} A_i$ مجموع مستقیم (خارجی) آن است. هرگاه مجموعهٔ اندیسگذار متناهی باشد، مثلاً $I = \{1,2,\ldots,n\}$، آنگاه حاصل‌ضرب مستقیم و مجموع مستقیم یکی هستند و به صورت $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ نوشته می‌شوند. نگاشتهای π_k [ι_k] تصاویر کانونی [انژکسیونها] نامیده می‌شوند.

قضیهٔ ۱۲۰۱. هرگاه R یک حلقه، $\{A_i \mid i \in I\}$ خانواده‌ای از R مدولها، C یک R ــ مدون، و $\{\varphi_i : C \to A_i \mid i \in I\}$ خانواده‌ای از همریختیهای R ــ مدولها باشد، آنگاه یک همریختی منحصر به فرد R ــ مدولها مانند $\varphi : C \to \prod_{i\in I} A_i$ وجود دارد به‌طوری‌که به‌ازای هر $i \in I$، $\pi_i\varphi = \varphi_i$. این خاصیت $\prod_{i\in I} A_i$ را با تقریب یکریختی به طور منحصر به فرد معین می‌کند. به عبارت دیگر، $\prod_{i\in I} A_i$ یک حاصل‌ضرب در رستهٔ R ــ مدولهاست.

برهان. بنابرقضیهٔ I ۲۰۸۰، یک‌همریختی منحصربه‌فرد از گروهها مانند $\varphi : C \to \prod A_i$ با خاصیت مطلوب وجود دارد که به وسیلهٔ $\varphi(c) = \{\varphi_i(c)\}_{i\in I}$ تعریف می‌شود. چون هر φ_i یک همریختی R ــ مدولهاست، $\varphi(rc) = \{\varphi_i(rc)\}_{i\in I} = \{r\varphi_i(c)\}_{i\in I} = r\{\varphi_i(c)\}_{i\in I} = r\varphi(c)$،

و φ یک همریختی R ــ مدولها می‌باشد. لذا، $\prod A_i$ یک حاصل‌ضرب در رستهٔ R ــ مدولهاست (تعریف I ۲۰۷۰)؛ و لذا، طبق قضیهٔ I ۳۰۷۰، با تقریب یکریختی معین است.

قضیهٔ I ۱۳۰۱. *هرگاه R یک حلقه، $\{A_i \mid i \in I\}$ خانواده‌ای از R ــ مدولها، D یک R ــ مدول، و $\{\psi_i : A_i \to D \mid i \in I\}$ خانواده‌ای از همریختیهای R ــ مدولها باشد، آنگاه یک همریختی منحصر به فرد از R ــ مدولها مانند $\psi : \sum_{i \in I} A_i \to D$ وجود دارد به‌طوری‌که به‌ازای هر $i \in I$، $\psi \iota_i = \psi_i$. این خاصیت $\sum_{i \in I} A_i$ را با تقریب یکریختی به طور منحصر به‌فرد معین می‌کند. به عبارت دیگر، $\sum_{i \in I} A_i$ یک هم‌حاصل‌ضرب در رستهٔ R ــ مدولهاست.*

برهان. بنابر قضیهٔ I ۵۰۸۰، همریختی منحصر به فردی از گروههای آبلی مانند $\psi : \sum A_i \to D$ با خاصیت مطلوب وجوددارد که $\psi(\{a_i\}) = \sum \psi_i(a_i)$ داده می‌شود، که در آن مجموع روی مجموعهٔ متناهی اندیسهای i گرفته شده است که $a_i \neq 0$. به آسانی معلوم می‌شود که ψ یک نگاشت R ــ مدول است. از اینرو، $\sum A_i$ یک هم‌حاصل‌ضرب در رستهٔ R ــ مدولهاست (تعریف I ۴۰۷۰)؛ و لذا، طبق قضیهٔ I ۵۰۷۰، با تقریب یکریختی معین می‌باشد.

مجموعهای مستقیم متناهی آنقدر پیش می‌آیند که توصیف بیشتر آنها مفید است. ابتدا می‌بینیم هرگاه f و g همریختیهای R ــ مدولها از R ــ مدول A به R ــ مدول B باشد، آنگاه نگاشت $f+g : A \to B$ داده شده با $a \mapsto f(a) + g(a)$ نیز یک همریختی R ــ مدولهاست. به آسانی تحقیق می‌شود که مجموعهٔ $\mathrm{Hom}_R(A,B)$ مرکب از تمام همریختیهای R ــ مدولهای $A \to B$ تحت‌این جمع یک گروه آبلی است (تمرین ۷). به علاوه، جمع همریختیهای مدولها نسبت به ترکیب توابع پخشپذیر است؛ یعنی،

$$h(f+g) = hf + hg \quad \text{و} \quad (f+g)k = fk + gk,$$

که در آنها $f,g : A \to B, h : B \to C, k : D \to A$.

قضیهٔ I ۱۴۰۱. *فرض کنیم R یک‌حلقه‌بوده‌و $A, A_1, A_2, \ldots, A_n$، R ــ مدولهایی باشند.*

در این صورت، $A \cong A_1 \oplus A_2 \oplus \cdots \oplus A_n$ **اگر و فقط اگر به‌ازای هر** $i = 1,2,\ldots,n$، **همریختیهایی از** R **ـ مدولها مانند** $\pi_i : A \to A_i$ **و** $\iota_i : A_i \to A$ **موجود باشند به‌طوری‌که**

(یک) **به‌ازای** $i = 1,2,\ldots,n$، $\pi_i\iota_i = 1_{A_i}$؛

(دو) **به‌ازای** $i \neq j$، $\pi_j\iota_i = 0$؛

(سه) $\iota_1\pi_1 + \iota_2\pi_2 + \cdots + \iota_n\pi_n = 1_A$.

برهان. ($\Leftarrow$) هرگاه A مدول $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ باشد، آنگاه می‌توان تحقیق کرد که انژکسیونهای ι_i و تصاویر π_i درشرایط (یک) تا (سه) صدق می‌کنند. به همین ترتیب، هرگاه تحت یکریختی $f: A \to A_1 \oplus \cdots \oplus A_n$ داشته باشیم $A \cong A_1 \oplus \cdots \oplus A_n$، آنگاه همریختیهای $\pi_i f: A \to A_i$ و $f^{-1}\iota_i : A_i \to A$ در شرایط (یک) تا (سه) صدق می‌کنند.
($\Rightarrow$) فرض کنیم $\pi_i : A \to A_i$ و $\iota_i : A_i \to A$ $(i = 1,2,\ldots,n)$ در شرایط (یک) تا (سه) صدق کنند. همچنین، $\pi_i' : A_1 \oplus \cdots \oplus A_n \to A_i$ و $\iota_i' : A_i \to A_1 \oplus \cdots \oplus A_n$ تصاویر کانونی‌وانژکسیونهاباشند. و نیز $\varphi : A_1 \oplus \cdots \oplus A_n \to A$ با $\varphi = \iota_1\pi_1' + \iota_2\pi_2' + \cdots + \iota_n\pi_n'$ و $\psi : A \to A_1 \oplus \cdots \oplus A_n$ با $\iota_1'\pi_1 + \iota_2'\pi_2 + \cdots + \iota_n'\pi_n$ داده شده باشد. در این صورت،

$$\varphi\psi = \left(\sum_{i=1}^{n} \iota_i\pi_i'\right)\left(\sum_{j=1}^{n} \iota_j'\pi_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \iota_i\pi_i'\iota_j'\pi_j = \sum_{i=1}^{n} \iota_i\pi_i'\iota_i'\pi_i$$

$$= \sum_{i=1}^{n} \iota_i 1_{A_i}\pi_i = \sum_{i=1}^{n} \iota_i\pi_i = 1_A.$$

به همین نحو، $\psi\varphi = \sum_{i=1}^{n}\sum_{j=1}^{n} \iota_i'\pi_i\iota_j\pi_j' = \sum_{i=1}^{n} \iota_i'\pi_i' = 1_{A_1 \oplus \ldots \oplus A_n}$. بنابراین، طبق قضیهٔ ۳۰۲۰ I، φ یک یکریختی است.

قضیهٔ ۱۵۰۱. **فرض کنیم** R **یک‌حلقه‌و** $\{A_i \mid i \in I\}$ **خانواده‌ای‌اززیرمدولهای** R **ـ مدول** A **باشد به‌طوری که**

(یک) A **مجموع خانوادهٔ** $\{A_i \mid i \in I\}$ **است؛**

(دو) **به‌ازای هر** $k \in I$، $A_k \cap A_k^* = 0$، **که‌درآن** A_k^* **مجموع خانوادهٔ** $\{A_i \mid i \neq k\}$ **است.**

در این صورت، یک یکریختی مانند $A \cong \sum_{i\in I} A_i$ **وجود دارد.**

برهان. تمرین؛ ر.ک. قضیهٔ I ۶.۸۰.

گوییم مدول A مجموع مستقیم *(داخلی)* خانوادهٔ $\{A_i \mid i \in I\}$ از زیرمدولهاست مشروط بر اینکه A و $\{A_i\}$ در مفروضات قضیهٔ ۱۵.۱ صدق کنند. مثل حالت گروهها، تمایزی بین مجموعهای مستقیم داخلی و خارجی وجود دارد هرگاه مدول A مجموع مستقیم *داخلی* مدولهای A_i باشد، آنگاه، طبق تعریف، هر A_i زیرمدولی از A است و A با مجموع مستقیم *خارجی* $\sum_{i\in I} A_i$ **یکریخت** است. با اینحال، مجموع مستقیم خارجی $\sum_{i\in I} A_i$ شامل مدولهای A_i **نیست**، بلکه فقط شامل نسخه‌های یکریخت آنهاست (یعنی، $\iota_i(A_i)$ ها ــ ر.ک. قضیهٔ ۱۱.۱ و تمرین I ۱۰.۸۰). چون این تمایز عملاً مهم نیست، وقتی از قراین روشن باشد، صفات "داخلی" و "خارجی" حذف می‌شوند و نماد زیر به کار خواهد رفت.

نمادگذاری. برای آنکه نشان دهیم مدول A مجموع مستقیم داخلی خانوادهٔ $\{A_i \mid i \in I\}$ از زیرمدولهاست، می‌نویسیم $A = \sum_{i\in I} A_i$.

تعریف ۱۶.۱. یک جفت از همریختیهای مدولها مانند $A \xrightarrow{f} B \xrightarrow{g} C$ را *کامل* در B گوییم مشروط بر آنکه $Im\, f = Ker\, g$. یک دنبالهٔ متناهی از همریختیهای مدولها مانند $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$ را *کامل* گوییم مشروط بر اینکه به‌ازای $i = 1, 2, \ldots, n-1$، $Im\, f_i = Ker\, f_{i+1}$. یک دنبالهٔ نامتناهی از همریختیهای مدولها مانند $\cdots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots$ را *کامل* گوییم مشروط بر اینکه به‌ازای هر $i \in Z$، $Im\, f_i = Ker\, f_{i+1}$.

در مواقع مقتضی کمی نادقیق شده و به جای دنبالهٔ کامل از همریختیهای مدولها دنبالهٔ کامل از مدولها خواهیم گفت.

چند مثال. ابتدا توجه کنید که به‌ازای هر مدول A، همریختیهای منحصر به فرد $0 \to A$

و $0 \to A$ ازمدولها وجود دارند. هرگاه A و B مدولهایی باشند، آنگاه دنباله‌های $0 \to B \xrightarrow{\pi} A \oplus B \xrightarrow{i} A \to 0$ و $0 \to A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \to 0$ کاملند، که در آنها i ، π ها به ترتیب انژکسیونها و تصاویر کانونی می‌باشند. به همین نحو، هرگاه C زیرمدول D باشد، آنگاه دنباله‌ٔ $0 \to C \xrightarrow{i} D \xrightarrow{p} D/C \to 0$ کامل است، که در آن i نگاشت شمول و p بروریختی کانونی است. هرگاه $f: A \to B$ یک همریختی مدولها باشد، آنگاه $A/\mathrm{Ker}\, f$ [$B/\mathrm{Im}\, f$] هم نقش f [هم هستهٔ f] نام داشته و با $\mathrm{Coim}\, f$ [$\mathrm{Coker}\, f$] نموده می‌شود. هر یک از دنباله‌های زیر کامل است: $0 \to \mathrm{Ker}\, f \to A \to \mathrm{Coim}\, f \to 0$ ، $0 \to \mathrm{Im}\, f \to B \to \mathrm{Coker}\, f \to 0$ ، و $0 \to \mathrm{Ker}\, f \to A \xrightarrow{f} B \to \mathrm{Coker}\, f \to 0$ ، که در آنها نگاشتهای بی‌نام شمولها و تصاویر می‌باشند.

چند تبصره. $0 \to A \xrightarrow{f} B$ یک دنباله‌ٔ کامل از همریختیهای مدولهاست اگر و فقط اگر f یک همریختی مدولها باشد. به همین نحو، $B \xrightarrow{g} C \to 0$ کامل است اگر و فقط اگر g یک بروریختی مدولها باشد. هرگاه $A \xrightarrow{f} B \xrightarrow{g} C$ کامل باشد، آنگاه $gf = 0$. بالاخره، هرگاه $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ کامل باشد، آنگاه $\mathrm{Coker}\, f = B/\mathrm{Im}\, f = B/\mathrm{Ker}\, g = \mathrm{Coim}\, g \cong C$. هر دنباله‌ٔ کامل به شکل $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ یک **دنباله‌ٔ کامل کوتاه** نام دارد؛ توجه کنید که f یک تکریختی و g یک بروریختی است. تبصره‌های پیشین نشان می‌دهند که یک دنباله‌ٔ کامل کوتاه راه دیگری برای نمایش یک زیرمدول ($A \cong \mathrm{Im}\, f$) و مدول خارج قسمتی آن ($B/\mathrm{Im}\, f = B/\mathrm{Ker}\, g \cong C$) است.

لم ۱۷۰۱ (لم پنج کوتاه). *فرض کنیم R حلقه بوده و*

$$\begin{array}{ccccccccc} 0 & \to & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \to & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \to & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \to & 0 \end{array}$$

یک نمودار تعویضپذیر از R ــ مدولها و همریختیهای R ــ مدولها باشد به‌طوری‌که هر سطر یک دنباله‌ٔ کامل کوتاه است. در این صورت،

(یک) β *تکریختی است* $\Rightarrow$ α, γ *تکریختی؛*

(دو) β *بروریختی است* $\Rightarrow$ α, γ *بروریختی؛*

(سه) β *یکریختی است* $\Rightarrow$ α, γ *یکریختی.*

برهان. (یک) فرض کنیم $b \in B$ و $\beta(b) = 0$؛ باید نشان دهیم که $b = 0$. بنابر تعویضپذیری، داریم

$$\gamma g(b) = g'\beta(b) = g'(0) = 0.$$

این ایجاب می‌کند که $g(b) = 0$، زیرا γ یک تکریختی است. بنابر کامل بودن سطر بالا در B، داریم $b \in \operatorname{Ker} g = \operatorname{Im} f$؛ مثلاً "، $b = f(a), a \in A$. بنابر تعویضپذیری،

$$f'\alpha(a) = \beta f(a) = \beta(b) = 0.$$

بنابر کامل بودن سطر پایین در A'، f' یک تکریختی است (قضیهٔ ۳.۲۰ I (یک))؛ از اینرو، $\alpha(a) = 0$. اما α یک تکریختی است؛ بنابراین، $a = 0$؛ و درنتیجه، $b = f(a) = f(0) = 0$. لذا، β یک تکریختی می‌باشد.

(دو) فرض کنیم $b' \in B'$. پس $g'(b') \in C'$؛ چون γ بروریختی است، به‌ازای $c \in C$ ای، $g'(b') = \gamma(c)$. بنابر کامل بودن سطر بالا در C، g بروریختی است؛ از اینرو، به‌ازای $b \in B$ ای، $c = g(b)$. بنابر تعویضپذیری،

$$g'\beta(b) = \gamma g(b) = \gamma(c) = g'(b').$$

لذا، $g'[\beta(b) - b'] = 0$ و، بنابر کامل بودن، $\beta(b) - b' \in \operatorname{Ker} g' = \operatorname{Im} f'$؛ مثلاً "، $f'(a') = \beta(b) - b', a' \in A'$. چون α بروریختی است، به‌ازای $a \in A$ ای، $a' = \alpha(a)$. $b - f(a) \in B$ را درنظر می‌گیریم:

$$\beta[b - f(a)] = \beta(b) - \beta f(a).$$

بنابر تعویضپذیری، $\beta f(a) = f'\alpha(a) = f'(a') = \beta(b) - b'$؛ از اینرو،

$$\beta[b - f(a)] = \beta(b) - \beta f(a) = \beta(b) - (\beta(b) - b') = b'$$

و β یک بروریختی است.

قسمت (سه) فوراً " از (یک) و (دو) نتیجه می‌شود.

دو دنبالهٔ کامل کوتاه را **یکریخت** گوییم اگر نمودار تعویضپذیری از همریختیهای مدولها مانند

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

موجود باشد به‌طوری‌که f، g، و h یکریختی باشند. در این حالت، به آسانی تحقیق

می‌شود که نمودار

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \uparrow{\scriptstyle f^{-1}} & & \uparrow{\scriptstyle g^{-1}} & & \uparrow{\scriptstyle h^{-1}} & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

(با همان‌نگاشتهای‌افقی) نیز تعویضپذیر است. در واقع، یکریختی دنباله‌های کامل کوتاه یک رابطهٔ هم‌ارزی است (تمرین ۱۴).

قضیهٔ ۱۸۰۱. *فرض کنیم* R *حلقه بوده و* $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ *یک دنبالهٔ کامل کوتاه از همریختیهای* R *ـ مدولها باشد. در این صورت، شرایط زیر معادل خواهند بود:*

(یک) یک همریختی R *ـ مدولها مانند* $h : A_2 \to B$ *وجود دارد که* $gh = 1_{A_2}$؛

(دو) یک همریختی R *ـ مدولها مانند* $k : B \to A_1$ *وجود دارد که* $kf = 1_{A_1}$؛

(سه) دنبالهٔ داده شده (با نگاشتهای همانی بر A_1 *و* A_2*) با مجموع مستقیم دنبالهٔ کامل کوتاه* $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$ *یکریخت است؛ بخصوص،* $B \cong A_1 \oplus A_2$.

گوییم یک دنبالهٔ کامل کوتاه صادق در شرایط معادل قضیهٔ ۱۸۰۱ **تجزیه می‌شود** یا یک *دنبالهٔ کامل* **تجزیه** می‌باشد.

طرح برهان ۱۸۰۱. (سه) $\Rightarrow$ (یک) بنابر قضیهٔ ۱۳۰۱، همریختیهای f و h یک همریختی مدولها مانند $\varphi : A_1 \oplus A_2 \to B$ را القا می‌کنند که با $(a_1,a_2) \mapsto f(a_1) + h(a_2)$ داده می‌شود. تحقیق کنید که نمودار

$$\begin{array}{ccccccccc} 0 & \to & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \to & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0 \end{array}$$

تعویضپذیر است (از این استفاده کنید که $gf = 0$ و $gh = 1_{A_2}$). بنابر لم پنج کوتاه، φ یک یکریختی است.

(سه) $\Rightarrow$ (دو) نمودار

$$\begin{array}{ccccccccc} 0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \to & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \to & 0 \end{array}$$

تعویضپذیراست، که درآن ψ یک همریختی مدولهای داده شده با $\psi(b) = (k(b),g(b))$ است (ر.ک. قضیه ۱۲.۱) . از اینرو، لم پنج کوتاه ایجاب می‌کند که ψ یک یکریختی باشد .

(یک) و (دو) $\Rightarrow$ (سه) فرض کنیم یک نمودار تعویضپذیر با سطرهای کامل داده شده باشد و φ یک یکریختی باشد :

$$\begin{array}{ccccccccc} 0 & \to & A_1 & \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} & A_1 \oplus A_2 & \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} & A_2 & \to & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0, \end{array}$$

$h : A_2 \to B$ را مساوی $\varphi\iota_2$ و $k : B \to A_1$ را برابر $\pi_1\varphi^{-1}$ تعریف می‌کنیم . با استفاده از تعویضپذیری نمودار و اینکه $\pi_i\iota_i = 1_{A_i}$, $\varphi^{-1}\varphi = 1_{A_1 \oplus A_2}$ ، نشان دهید که $kf = 1_{A_1}$ و $gh = 1_{A_2}$.

تمرینات

تذکر. R یک حلقه است .

۱ . هرگاه A یک گروه آبلی بوده و $n > 0$ عددی صحیح باشد به‌طوری‌که به‌ازای هر $a \in A$ ، $na = 0$ ، آنگاه A یک Z_n ــ مدول یکانی است که عمل Z_n بر A با $\bar{k}a = ka$ داده می‌شود ، که درآن $k \in \mathbf{Z}$ و $k \mapsto \bar{k} \in Z_n$ تحت تصویر کانونی $\mathbf{Z} \to Z_n$ است .

۲ . فرض کنید $f : A \to B$ یک همریختی R ــ مدولها باشد .

(آ) f تکریختی است اگر و فقط اگر به‌ازای هر جفت همریختی R ــ مدولها مانند $g,h : D \to A$ که $fg = fh$ ، داشته باشیم $g = h$. [**راهنمایی.** برای اثبات ($\Rightarrow$) ، فرض کنید $D = \operatorname{Ker} f$ و نگاشت شمول و h نگاشت صفر باشد .]

(ب) f یک بروریختی است اگر و فقط اگر به ازای هر جفت همریختی R مدولها مانند $k,t : B \to C$ به طوری که $kf = tf$ ، داشته باشیم $k = t$. [**راهنمایی.** برای اثبات ($\Leftarrow$) فرض کنید k بروریختی کانونی $B \to B/\operatorname{Im} f$ و t نگاشت صفر باشد .]

۳ . فرض کنید I ایده‌آل چپ حلقه R بوده و A یک R ــ مدول باشد .

(آ) هرگاه S زیرمجموعه‌ای ناتهی از A باشد ، آنگاه

$$IS = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbf{N}^*; r_i \in I; a_i \in S \right\}$$

یک زیرمدول A است. توجه کنید که هرگاه $S = \{a\}$، آنگاه $IS = Ia = \{ra \mid r \in I\}$.

(ب) هرگاه I ایده‌آلی دوطرفه باشد، آنگاه A/IA یک R/I ــ مدول است که عمل R/I با $(r + I)(a + IA) = ra + IA$ داده می‌شود.

۴. هرگاه R یکدار باشد، آنگاه هر R ــ مدول دوری یکانی با R ــ مدولی به شکل R/J یکریخت است، که در آن J یک ایده‌آل چپ R است.

۵. هرگاه R یکدار باشد، آنگاه R ــ مدول یکانی ناصفر A **ساده** است اگر زیرمدولهای آن فقط 0 و A باشند.

(آ) هر R ــ مدول ساده دوری است.

(ب) اگر A ساده باشد، هر درونریختی R ــ مدولها یا نگاشت صفر است یا یکریختی.

۶. یک R ــ مدول با تولید متناهی لزوماً یک گروه آبلی با تولید متناهی نیست. [**راهنمایی.** تمرین II ۱۰۱۰۰]

۷. (آ) هرگاه A و B، R ــ مدول باشند، آنگاه مجموعهٔ $\mathrm{Hom}_R(A,B)$ مرکب از تمام همریختیهای R ــ مدولها از A به توی B یک گروه آبلی است که اثر $f + g$ بر $a \in A$ با $(f + g)(a) = f(a) + g(a) \in B$ داده می‌شود. عنصر همانی نگاشت صفر می‌باشد.

(ب) $\mathrm{Hom}_R(A,A)$ یک حلقهٔ یکدار است، که در آن ضرب ترکیب توابع است. $\mathrm{Hom}_R(A,A)$ **حلقهٔ درونریختی** A نام دارد.

(پ) A یک $\mathrm{Hom}_R(A,A)$ ــ مدول چپ است که در آن fa با

$$f(a)\ (a \in A, f \in \mathrm{Hom}_R(A,A))$$

تعریف شده است.

۸. ثابت کنید مشابه‌های واضح قضیهٔ I ۱۰۰۸۰ و نتیجهٔ I ۱۱۰۸۰ برای R ــ مدولها برقرار است.

۹. هرگاه $f : A \to A$ یک همریختی R ــ مدولها باشد به‌طوری‌که $ff = f$، آنگاه

$$A = \mathrm{Ker}\, f \oplus \mathrm{Im}\, f.$$

۱۰. فرض کنید $A, A_1, \ldots, A_n$، R ــ مدول باشند. در این صورت، $A \cong A_1 \oplus \cdots \oplus A_n$ اگر و فقط اگر به‌ازای هر $i = 1,2,\ldots,n$، یک همریختی R ــ مدولها مانند $\varphi_i : A \to A$ موجود باشد به‌طوری‌که $\varphi_i \varphi_j = 0$؛ به‌ازای $i \neq j$، $\mathrm{Im}\ \varphi_i \cong A_i$;

$A \cong A_1 \oplus \cdots \oplus A_n$ اگر **راهنمایی.**] . $\varphi_1 + \varphi_2 + \cdots + \varphi_n = 1_A$ و $\varphi_i\varphi_j = 0$ ؛ π_i, ι_i ها را مثل قضیهٔ ۱۴۰۱ گرفته و تعریف کنید $\varphi_i = \iota_i\pi_i$. بـه عکس، به‌ازای $\{\varphi_i\}$ داده شده، نشان دهید که $\varphi_i = \varphi_i\varphi_i$. فرض کنید $\psi_i = \varphi_i \mid \operatorname{Im}\varphi_i : \operatorname{Im}\varphi_i \to A$ و قضیهٔ ۱۴۰۱ را با A ، $\operatorname{Im}\varphi_i$ ، φ_i ، و ψ_i به جای A ، A_i ، π_i ، و ι_i بـه کار برید . [

۱۱ . (آ) هـرگـاه A یک مـدول روی حلقـهٔ تعـویضپذیر R بـوده و $a \in A$ ، آنگاه $\mathcal{O}_a = \{r \in R \mid ra = 0\}$ ایـده‌آلی از R است . اگر $\mathcal{O}_a \neq 0$ ، گوییم a یک **عنصر تابی** A است .

(ب) هرگاه R دامنهٔ صحیح باشد ،آنگاه مجموعهٔ $T(A)$ مرکب از تمام عناصرتابی A یک زیرمدول A است . ($T(A)$ **زیرمدول تابی** نام دارد .)

(پ) نشـان دهیـد (ب) ممکن است برای حلقهٔ تعویضپذیر R که دامنهٔ صحیح نیست درست نباشد .

از (ت) تا (ج) R یک دامنهٔ صحیح است .

(ت) هرگاه $f : A \to B$ یک همریختی R ــ مدولها باشد ، آنگاه $f(T(A)) \subset T(B)$ ؛ از اینرو ، f_T ، تحدید f به $T(A)$ ،یک‌همریختی R ــ مدولها از $T(A)$ به $T(B)$ است .

(ث) هرگاه $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ یک دنبـالهٔ کـامل از R ــ مـدولها باشد ، آنگاه $0 \to T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C)$ نیز چنین است .

(ج) هرگاه $g : B \to C$ یک بروریختی R ــ مدولهاباشد ، آنگاه $g_T : T(B) \to T(C)$ لزوما" یـک بروریختی نیست . [**راهنمایی.** گروههای آبلی را درنظر بگیرید .]

۱۲ . (لم پنج) . فرض کنید

$$\begin{array}{ccccccccc} A_1 & \to & A_2 & \to & A_3 & \to & A_4 & \to & A_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ B_1 & \to & B_2 & \to & B_3 & \to & B_4 & \to & B_5 \end{array}$$

یک نمودارتعویضپذیر از R ــ مدولها و همریختیهای R ــ مدولها با سطرهای کامل باشد . ثابت کنید که

(آ) α_3 تکریختی $\Rightarrow$ α_1 بروریختی و α_2, α_4 تکریختی ؛

(ب) α_3 بروریختی $\Rightarrow$ α_5 تکریختی و α_2, α_4 بروریختی .

۱۳ . (آ) هرگاه $0 \to A \to B \xrightarrow{f} C \to 0$ و $0 \to C \xrightarrow{g} D \to E \to 0$ دنباله‌های‌کامل‌کوتاهی

از مدولها باشند ، آنگاه دنباله‌ٔ $0 \to A \to B \xrightarrow{gf} D \to E \to 0$ کامل است .

(ب) نشان دهید که هر دنباله‌ٔ کامل را می‌توان با به هم بافتن دنباله‌های کامل کوتاه مناسبی چون (آ) به دست آورد .

۱۴ . نشان دهید که یکریختی دنباله‌های کامل کوتاه یک رابطهٔ هم‌ارزی است .

۱۵ . هرگاه $f : A \to B$ و $g : B \to A$ همریختیهایی از R ــ مدولها باشند به‌طوری که $gf = 1_A$ ، آنگاه $B = \operatorname{Im} f \oplus \operatorname{Ker} g$.

۱۶ . فرض کنید R یک حلقه و R^{op} حلقهٔ متقابل آن باشد (تمرین III ۷.۱۰) . هرگاه A یک R ــ مدول چپ [راست]باشد ، آنگاه A یک R^{op} مدول راست [چپ] است به‌طوری که به‌ازای هر $a \in A, r \in R, r \in R^{op}$ ، $ra = ar$.

۱۷ . (آ) هرگاه R یکدار بوده و A یک R ــ مدول باشد ، آنگاه زیرمدولهایی مانند B و C از A وجود دارند به‌طوری‌که B یکانی است ، $RC = 0$ ، و $A = B \oplus C$.
[**راهنمایی** . فرض کنید $B = \{1_R a \mid a \in A\}$ و $C = \{a \in A \mid 1_R a = 0\}$ و توجه کنید که به‌ازای هر $a \in A$ ، $a - 1_R a \in C$.]

(ب) فرض کنید A_1 ، R ــ مدول دیگری باشد که $A_1 = B_1 \oplus C_1$ (B_1 یکانی است ، $RC_1 = 0$) . هرگاه $f : A \to A_1$ یک همریختی R ــ مدولها باشد ، آنگاه $f(B) \subset B_1$ و $f(C) \subset C_1$.

(پ) هرگاه نگاشت f قسمت (ب) یک برووریختی [یکریختی] باشد ، آنگاه $f \mid B : B \to B_1$ و $f \mid C : C \to C_1$ نیز چنین‌اند .

۱۸ . فرض کنید R حلقه‌ای بدون‌واحد باشد . همانند در برهان قضیهٔ III ۱۰.۱۰ ، R را در حلقهٔ یکدار S با مشخص صفر بنشانید و R را با نقش خود در S یکی کنید .
(آ) نشان دهیدکه هر عنصر S را می‌توان به‌طور منحصر به فرد به شکل $r1_S + n1_S$ $(r \in R, n \in \mathbb{Z})$ بیان کرد .

(ب) اگر A یک R ــ مدول بوده و $a \in A$ ، نشان دهید که یک همریختی منحصر به فرد از R ــ مدولها مانند $f : S \to A$ وجود دارد به‌طوری‌که $f(1_S) = a$.
[**راهنمایی** . فرض کنید $f(r1_S + n1_S) = ra + na$.]

۲ مدولهای آزاد و فضاهای برداری

در این بخش به مطالعه اشیاء آزاد در رستهٔ مدولها روی یک حلقه می‌پردازیم . این

مـــدولهای آزاد ، که مهمترینشان فضاهای برداری روی یک حلقهٔ بخشی‌اند (قضیهٔ ۴۰۲) ، دارای کاربردهای وسیعی در بسیاری از حیطه‌های ریاضی می‌باشند . حالت خاص گروههای آبلی آزاد ($\mathbf{Z}$ ــ مدولها) مدلی برای قسمت اول این بخش است . بقیهٔ بخش به بحثی از بعد (یا رتبهٔ) یک مدول آزاد (قضایای ۶۰۲ تا ۱۲۰۲) و بررسی خواص ویژهٔ بعد یک فضای برداری (قضایا و نتایج ۱۳۰۲ تا ۱۶۰۲) اختصاص دارد .

زیـرمجمـوعهٔ X از R ــ مـدول A را **مستقـل خطـی** گوییم درصورتی‌که به‌ازای $x_1, \ldots, x_n \in X$ متمایز و $r_i \in R$ ،

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0 \Rightarrow r_i = 0 \text{ ، } i \text{ به‌ازای هر}$$

مجمـوعه‌ای کـه مستقل خطـی نبـاشد **وابستهٔ خطی** نام دارد . هرگاه A به عنوان یک R ــ مدول بـه وسیلهٔ مجموعهٔ Y تولید شده باشد ، آنگاه گوییم Y ، A را **می‌پیماید** . اگر R یکدار بـوده و A یکانی باشد ، Y ، A را می‌پیماید اگر و فقط اگر هر عنصر A را بتوان به صورت ترکیبی خطی مانند $r_1y_1 + r_2y_2 + \cdots + r_ny_n$ $(r_i \in R, y_i \in Y)$ بیان کرد ؛ ر.ک. قضیهٔ ۵۰۱ . یک زیرمجموعهٔ مستقل خطی از A که A را بپیماید یک **پایهٔ** A نام دارد . تـوجه کنید که مجموعهٔ تهی (به‌طور خالی) مستقل خطی است و یک پایهٔ مدول صفر می‌باشد (ر.ک. تعریف ۴۰۱) .

قضیهٔ ۱۰۲ . *فرض کنیم R حلقه‌ای یکدار باشد . شرایط زیر بر R ــ مدول یکانی F با هم معادلند :*

(یک) F دارای پایه‌ای ناتهی است ؛

(دو) F مجموع مستقیم داخلی خـانواده‌ای از R ــ مدولهای دوری است که هر یک به عنوان R ــ مدول چپ با R یکریخت است ؛

(سه) F با مجموع مستقیم نسخه‌هایی از R ــ مدول چپ R یکریخت R ــ مدولهاست ؛

(چهار) مجموعهٔ نـاتهی X و تابع $\iota : X \to F$ ، با خاصیت زیر وجود دارند : به‌ازای هر R ــ مـدول یـکانی A و تابع $f : X \to A$ ، همریختی منحصر به فردی از R ــ مدولها مـانـنـد $\bar{f} : F \to A$ وجـود دارد بـه‌طوری که $\bar{f}\iota = f$. به عبارت دیگر ، F در رسـتـهٔ R ــ مدولهای یکانی یک شیٔ آزاد است .

قضیه ذیـلا " ثـابت شده است . مدول یکانی F روی حلقهٔ یکدار R که در شرایط

معادل قضیهٔ ۱۰۲ صدق کند یک R ــ **مدول آزاد** بر مجموعهٔ X نام دارد. بنابر قضیهٔ ۱۰۲ (چهار)، F یک شیء آزاد در رستهٔ تمام R ــ مدولهای چپ **یکانی** است. اما چنین F در رستهٔ **تمام** R ــ مدولهای چپ یک شیء آزاد **نیست** (تمرین ۱۵). طبق تعریف، مدول صفر مدول آزاد بر مجموعهٔ تهی است.

می‌توان مدولهای آزاد را در رستهٔ تمام R ــ مدولهای چپ روی حلقهٔ دلخواه R (احتمالاً "بدون واحد") تعریف کرد؛ ر.ک. تمرین ۲. یک چنین مدول آزاد با مجموع مستقیم نسخه‌های R، حتی وقتی که R یکدار باشد، یکریخت **نیست** (تمرین ۲). در موارد معدود زیر، نتایجی برای این مدولهای آزاد در رستهٔ تمام R ــ مدولهای چپ نیز برقرارند. با اینحال، اصطلاح "مدول آزاد" همواره به معنی مدول آزاد یکانی به مفهوم قضیهٔ ۱۰۲ است مگر خلافش تصریح شود.

طرح برهان ۱۰۲. (دو) $\Rightarrow$ (یک) فرض کنیم X پایه‌ای از F بوده و $x \in X$. نگاشت $R \to Rx$ داده‌شده با $r \mapsto rx$، طبق قضیهٔ ۵۰۱، یک بروریختی R ــ مدولهاست. هرگاه $rx = 0$، آنگاه، بنابر استقلال خطی، $r = 0$، که از آنجا نگاشت یک تکریختی بوده و، به‌عنوان R ــ مدولها، $R \cong Rx$. تحقیق کنید که F مجموع مستقیم داخلی مدولهای دوری Rx $(x \in X)$ است.

(سه) $\Rightarrow$ (دو) قضیهٔ ۱۵۰۱ و تمرین ۸۰۱.

(یک) $\Rightarrow$ (سه) فرض کنیم $F \cong \sum R$ و نسخه‌هایی از R به وسیلهٔ مجموعهٔ X اندیسگذاری شده باشند. به‌ازای هر $x \in X$، θ_x را عنصر $\{r_i\}$ از $\sum R$ می‌گیریم، که در آن به‌ازای $i \neq x$، $r_i = 0$ و $r_x = 1_R$. تحقیق کنید که $\{\theta_x \mid x \in X\}$ پایه‌ای از $\sum R$ است و، با استفاده از یکریختی $F \cong \sum R$، پایه‌ای از F به دست آورید.

(چهار) $\Rightarrow$ (یک) فرض کنیم X پایه‌ای از F بوده و $\iota : X \to F$ نگاشت شمول باشد. همچنین، نگاشت $f : X \to A$ داده‌شده باشد. هرگاه $u \in F$، آنگاه $u = \sum_{i=1}^{n} r_i x_i$ $(r_i \in R, x_i \in X)$، زیرا X، F را می‌پیماید. هرگاه $u = \sum_{i=1}^{n} s_i x_i$ $(s_i \in R)$، آنگاه $\sum_i (r_i - s_i)x_i = 0$، که از آنجا، طبق استقلال خطی، به‌ازای هر i، $r_i = s_i$. درنتیجه، نگاشت $\bar{f} : F \to A$ داده شده با

$$\bar{f}(u) = \bar{f}\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} r_i f(x_i)$$

تابع تعریف شده‌ای است به‌طوری‌که $\bar{f}\iota = f$. تحقیق کنید که $\bar{f}$ یک همریختی R ــ مدولهاست. چون X ، F را تولید می‌کند ،هرهمریختی R ــ مدولها مانند $F \to A$ به‌طورِ منحصر به فرد با عملش بر X معین می‌شود. لذا ، هرگاه $g : F \to A$ یک همریختی R ــ مدولها باشد به‌طوری‌که $g\iota = f$ ، آنگاه ، به‌ازای هر $x \in X$ ، $g(x) = g(\iota(x)) = f(x) = \bar{f}(x)$ ، که از آنجا $g = \bar{f}$ و $\bar{f}$ منحصر به فرد است. بنابراین، طبق تعریف I ۷۰۷۰ ، F یک شئ آزاد بر مجموعهٔ X در رستهٔ R ــ مدولهای یکانی است.

(سه) $\Rightarrow$ (چهار) به فرض آنکه $\iota : X \to F$ ، مجموع مستقیم $\sum R$ را ، به‌ازای هر x یک نسخه از R ،می‌سازیم . فرض کنیم $Y = \{\theta_x \mid x \in X\}$ پایه‌ای از R ــ مدول (یکانی) $\sum R$ مثل برهان (یک) $\Rightarrow$ (سه) باشد .برهان (چهار) $\Rightarrow$ (یک) $\Rightarrow$ (سه) نشان می‌دهدکه $\sum R$ یک شیٔ آزادبرمجموعهٔ Y دررستهٔ R ــ مدولهاست (با $Y \to \sum R$ نگاشت شمول) چون $|Y| = |X|$ ، برهان قضیهٔ I ۸۰۷۰ ایجاب می‌کند که یک یکریختی R ــ مدولها مانند $f : F \cong \sum R$ وجود داشته باشد به‌طوری‌که $f(\iota(X)) = Y$.

چند تبصره. (آ) هرگاه F یک R ــ مدول آزاد بر مجموعهٔ $X(\iota : X \to F)$ باشد ، آنگاه برهان (سه) $\Rightarrow$ (چهار) قضیهٔ ۱۰۲ ایجاب می‌کند که $\iota(X)$ درواقع یک پایه‌از F باشد.

(ب) به عکس، برهان (چهار) $\Rightarrow$ (یک) قضیهٔ ۱۰۲ نشان می‌دهد که هرگاه X یک پایه از مدول یکانی F روی حلقهٔ یکدار R باشد ، آنگاه F بر X آزاد است ، که $\iota : X \to F$ نگاشت شمول می‌باشد .

(پ) هرگاه X یک مجموعهٔ ناتهی و R حلقه‌ای یکدار باشد ، آنگاه برهان قضیهٔ ۱۰۲ طرز ساختن یک R ــ مدول آزاد بر مجموعهٔ X را نشان می‌دهد . کافی است فرض کنیم F مجموع مستقیم $\sum R$ باشدکه‌درآن نسخه‌های R با مجموعهٔ X اندیسگذاری شده‌اند . با نمادهای برهان ، $\{\theta_x \mid x \in X\}$ پایه‌ای‌از F است؛ درنتیجه ، $F = \sum_{x \in X} R\theta_x$. چون نگاشت $\iota : X \to F$ داده شده با $x \mapsto \theta_x$ انژکتیو است ، به آسانی معلوم می‌شود که F بر X به مفهوم شرط (چهار) قضیهٔ ۱۰۲ آزاد است . در این وضع ، معمولا " X را با نقش خود

تحت ، یکی کرده ، x را به جای θ_x می‌نویسیم ؛ درنتیجه ، $X \subset F$. با این نمادگذاری ، $F = \sum_{x \in X} R\theta_x$ به صورت $\sum_{x \in X} Rx$ نوشته می‌شود و عنصر نوعی F به شکل $r_1x_1 + \cdots + r_nx_n$ $(r_i \in R; x_i \in X)$ می‌باشد . بخصوص ، $X = \iota(X)$ پایه‌ای از F است .

(ت) وجود مدولهای آزاد بر یک مجموعه در رسته‌ٔ تمام مدولها روی یک حلقهٔ دلخواه (احتمالا " بدون واحد) در تمرین ۲ ثابت می‌شود .

نتیجهٔ ۲۰۲ . *هر مدول (یکانی) A روی حلقهٔ R (دارای واحد) نقش همریخت یک R ــ مدول آزاد مانند F است . هرگاه A با تولید متناهی باشد ، آنگاه F را می‌توان با تولید متناهی اختیار کرد .*

تبصره . اگر عبارات داخل پرانتزها حذف شده و "مدول آزاد" به معنی مدول آزاد در رستهٔ تمام مدولهای چپ روی یک حلقهٔ دلخواه (به صورت تعریف شده در تمرین ۲) گرفته شود ، نتیجهٔ ۲۰۲ و برهانش برقرارند .

***طرح برهان* ۲۰۲ .** فرض کنیم X مجموعه‌ای از مولدهای A بوده و F ، R ــ مدول آزاد بر مجموعهٔ X باشد . در این صورت ، نگاشت شمول $X \to A$ یک همریختی R ــ مدولها مانند $\bar{f} : F \to A$ القا می‌کند که $X \subset \operatorname{Im} \bar{f}$ (قضیهٔ ۱۰۲ (چهار)) . چون X ، A را تولید می‌کند ، باید داشته باشیم $\operatorname{Im} \bar{f} = A$.

تبصره . به خلاف وضع در مورد گروههای آبلی آزاد ، یک زیرمدول از یک مدول آزاد روی یک حلقهٔ دلخواه لزوما " آزاد نیست . مثلا " ، $\{0,2,4\}$ یک زیرمدول Z_6 است ، ولی بوضوح یک Z_6 ــ مدول آزاد نیست ؛ قضیهٔ II ۶.۱۰ را با قضیهٔ ۱۰۶ زیر مقایسه کنید .

فضاهای برداری روی حلقهٔ بخشی D (تعریف ۱۰۱) به جهاتی مهمند ازجمله اینکه **هر** فضای برداری روی D درواقع یک D ــ مدول آزاد است . برای اثبات این امر به لم زیر نیاز داریم .

لم ۳۰۲ . *زیرمجموعهٔ مستقل خطی ماکزیمال X از فضای برداری V روی حلقهٔ بخشی*

D پایه‌ای برای V است.

برهان. فرض کنیم W زیرفضایی از V باشد که به وسیلهٔ مجموعهٔ X پیموده شده است. چون X مستقل‌خطی بوده و W را می‌پیماید، X یک‌پایهٔ W است. اگر $W = V$، کار تمام است. اگر نباشد، عنصر ناصفری چون $a \in V$ وجود دارد که $a \notin W$. مجموعهٔ $X \cup \{a\}$ را درنظر می‌گیریم. هرگاه $ra + r_1x_1 + \cdots + r_nx_n = 0$ $(r, r_i \in D, x_i \in X)$ و $r \neq 0$، آنگاه $a = r^{-1}(ra) = -r^{-1}r_1x_1 - \cdots - r^{-1}r_nx_n \in W$، که با انتخاب a تعارض دارد. از اینرو، $r = 0$، که ایجاب می‌کند که به‌ازای هر i، $r_i = 0$، زیرا X مستقل خطی است. درنتیجه، $X \cup \{a\}$ یک زیرمجموعهٔ مستقل خطی از V است، که با ماکزیمالی X تعارض دارد. بنابراین، $W = V$ و X یک پایه می‌باشد.

قضیهٔ ۴۰۲. *هر فضای برداری V روی حلقهٔ بخشی D دارای پایه است؛ و لذا، یک D ــ مدول آزاد می‌باشد. به‌طورکلی، هر زیرمجموعهٔ مستقل خطی V مشمول پایه‌ای از V می‌باشد.*

عکس قضیهٔ ۴۰۲ نیز درست است؛ یعنی، هرگاه هر مدول یکانی روی حلقهٔ یکدار D آزاد باشد، آنگاه D یک حلقهٔ بخشی می‌باشد (تمرین ۱۴۰۳).

طرح برهان ۴۰۲. حکم اول نتیجهٔ فوری حکم دوم است، زیرا مجموعهٔ پوچ یک زیرمجموعهٔ مستقل‌خطی هرفضای برداری است. درنتیجه، فرض می‌کنیم X یک زیرمجموعهٔ مستقل خطی از V بوده و $\mathcal{S}$ مجموعهٔ تمام زیرمجموعه‌های مستقل‌خطی از V باشد که شامل X اند. چون $X \in \mathcal{S}$، $\mathcal{S} \neq \varnothing$. $\mathcal{S}$ را باشمول‌نظریهٔ مجموعه‌ها ترتیب جزئی می‌بخشیم. اگر $\{C_i \mid i \in I\}$ زنجیری در $\mathcal{S}$ باشد، تحقیق کنید که مجموعهٔ $C = \bigcup_{i \in I} C_i$ مستقل خطی است؛ و درنتیجه، عنصری از $\mathcal{S}$ می‌باشد. واضح است که C یک کران بالایی برای زنجیر $\{C_i \mid i \in I\}$ می‌باشد. بنابر لم زرن، $\mathcal{S}$ شامل عنصر ماکزیمال B است که حاوی X بوده و لزوماً یک زیرمجموعهٔ مستقل خطی ماکزیمال V می‌باشد. بنابر لم ۳۰۲، B پایه‌ای از V خواهد بود.

قضیهٔ ۵۰۲. *هرگاه V یک فضای برداری روی حلقهٔ بخشی D بوده و X زیرمجموعه‌ای*

باشد که V را می‌پیماید، آنگاه X شامل پایه‌ای از V می‌باشد.

طرح برهان. مجموعهٔ S مرکب‌ازتمام زیرمجموعه‌های مستقل خطی X را با شمول جزئی مرتب می‌کنیم. لم‌زرن‌وجود زیرمجموعهٔ مستقل خطی ماکزیمال Y از X را ایجاب می‌کند. هر عنصر X ترکیبی خطی از عناصر Y است (در غیر این صورت، همانند در لم ۳۰۲، می‌توانستیم زیرمجموعهٔ مستقل خطیی از X بسازیم که حقیقتا" مشمول Y باشد، که با ماکزیمالی متناقض می‌شد). چون X، V را می‌پیماید، Y نیز چنین می‌کند. از اینرو، Y پایه‌ای برای V خواهد بود.

در حالت گروههای آبلی آزاد ($\mathbf{Z}$ ـ مدولها) می‌دانیم که هر دو پایه از یک $\mathbf{Z}$ ـ مدول‌آزاددارای‌اصلیت یکسانند (قضیهٔ II ۲۰۱۰). متاسفانه، این برای مدولهای آزاد روی حلقه‌های یکدار دلخواه درست نیست (تمرین ۱۳). حال نشان‌می‌دهیم که فضاهای‌برداری‌روی‌حلقهٔ‌بخشی‌و مدولهای آزاد روی حلقهٔ تعویضپذیر یکدار این خاصیت را دارند.

قضیهٔ ۶۰۲. *فرض‌کنیم R حلقه‌ای یکدار بوده و F یک R ـ مدول آزاد با پایهٔ نامتناهی X باشد. در این صورت، هر پایهٔ F همان اصلیت X را خواهد داشت.*

برهان. هرگاه Y پایهٔ دیگری‌برای F باشد، آنگاه حکم می‌کنیم که Y نامتناهی است. فرض‌کنیم، به عکس، Y متناهی باشد. چون Y، F را تولید می‌کند و هر عنصر Y ترکیبی‌خطی‌از تعدادی متناهی از عناصر X می‌باشد، پس نتیجه می‌شود که زیرمجموعه‌ای متناهی مانند $\{x_1, \ldots, x_m\}$ از X وجود دارد که F را تولید می‌کند. چون X نامتناهی است، عنصری مانند

$$x \in X - \{x_1, \ldots, x_m\}$$

وجوددارد. دراین صورت، به‌ازای $r_i \in R$ ی، $x = r_1x_1 + \cdots + r_mx_m$، که استقلال خطی X را نقض می‌کند. بنابراین، Y نامتناهی می‌باشد.

فرض‌کنیم $K(Y)$ مجموعهٔ‌تمام‌زیرمجموعه‌های‌متناهی Y باشد. نگاشت $f : X \to K(Y)$

را با $x \mapsto (y_1, \ldots, y_n)$ تعریف می‌کنیم، که در آن $x = r_1y_1 + \cdots + r_ny_n$ و، به‌ازای هر i، $r_i \neq 0$. چون Y پایه است، y_i ها به‌طور منحصر به فرد معین شده و f یک تابع تعریف شده می‌باشد (که لزوماً انژکتیو نیست). هرگاه $\operatorname{Im} f$ متناهی می‌بود، آنگاه $\bigcup_{S \in \operatorname{Im} f} S$ زیرمجموعه‌ای متناهی از Y می‌شد که X، و درنتیجه F، را تولید می‌کرد. این امر، مثل‌بند پیش، به تناقضی با استقلال خطی Y منجر می‌شود. لذا، $\operatorname{Im} f$ نامتناهی می‌باشد.

حال نشان می‌دهیم که $T \in \operatorname{Im} f \subset K(Y)$ ، به‌ازای هر $f^{-1}(T)$ ، یک زیرمجموعهٔ متناهی X است. هرگاه $x \in f^{-1}(T)$ ، آنگاه x مشمول‌زیرمدول F_T از F است که به وسیلهٔ T تولید می‌شود؛ یعنی، $f^{-1}(T) \subset F_T$ (ر.ک. قضیهٔ ۵.۱). چون T متناهی است وهر $y \in T$ ترکیبی خطی از تعدادی متناهی از عناصر X است، زیرمجموعه‌ای متناهی از X مانند S وجود دارد به‌طوری‌که F_T مشمول زیرمدول F_S از F است که به وسیلهٔ S تولید می‌شود. لذا، $x \in f^{-1}(T)$ ایجاب می‌کندکه $x \in F_S$ و x ترکیبی خطی از عناصر S می‌باشد (قضیهٔ ۵.۱). چون $x \in X$ و $S \subset X$، این استقلال خطی X را نقض می‌کند مگر آنکه $x \in S$. بنابراین، $f^{-1}(T) \subset S$ ، که از آنجا $f^{-1}(T)$ متناهی می‌باشد.

به‌ازای هر $T \in \operatorname{Im} f$ ، عناصر $f^{-1}(T)$ را مرتب می‌کنیم، مثلاً $x_1, \ldots, x_n$ ، و نگاشت انژکتیو $g_T : f^{-1}(T) \to \operatorname{Im} f \times \mathbf{N}$ را با $x_k \mapsto (T,k)$ تعریف می‌کنیم. تحقیق کنیدکه مجموعه‌های $f^{-1}(T)$ $(T \in \operatorname{Im} f)$ افرازی از X را تشکیل می‌دهند. پس نتیجه می‌شود که نگاشت $X \to \operatorname{Im} f \times \mathbf{N}$ تعریف شده با $x \mapsto g_T(x)$ ، که $x \in f^{-1}(T)$ ، یک تابع انژکتیو تعریف شده است، که از آنجا $|X| \leq |\operatorname{Im} f \times \mathbf{N}|$. بنابراین، طبق تعریف ۳.۸، قضیهٔ ۱۱.۸، و نتیجهٔ ۱۳.۸ آشنایی،

$$|X| \leq |\operatorname{Im} f \times \mathbf{N}| = |\operatorname{Im} f|\,\aleph_0 = |\operatorname{Im} f| \leq |K(Y)| = |Y|.$$

تعویض‌باهم X و Y در استدلال فوق نشان می‌دهد که $|Y| \leq |X|$. بنابراین، طبق قضیهٔ شرودر ــ برنشتاین، $|Y| = |X|$.

قضیهٔ ۷.۲. *هرگاه V یک فضای برداری روی حلقهٔ بخشی D باشد، آنگاه هر دو پایهٔ V دارای یک اصلیت می‌باشند.*

برهان. فرض کنیم X و Y پایه‌هایی از V باشند. هرگاه X یا Y نامتناهی باشد، آنگاه

طبق قضیهٔ ۶۰۲ ، $|X| = |Y|$. از اینرو ، فرض می‌کنیم X و Y متناهی باشند ؛ مثلا " ، $X = \{x_1, \ldots, x_n\}$ و $Y = \{y_1, \ldots, y_m\}$. چون X و Y پایه‌اند ، به‌ازای $r_i \in D$ ی ، $0 \neq y_m = r_1x_1 + \cdots + r_nx_n$. هرگاه r_k اولین r_i ناصفر باشد ، آنگاه $x_k = r_k^{-1}y_m - r_k^{-1}r_{k+1}x_{k+1} - \cdots - r_k^{-1}r_nx_n$. بنابراین ، مجموعهٔ $X' = \{y_m, x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n\}$ ، V رامی‌پیماید (زیرا X چنین می‌کند) . بخصوص ،

$$y_{m-1} = s_my_m + t_1x_1 + \cdots + t_{k-1}x_{k-1} + t_{k+1}x_{k+1} + \cdots + t_nx_n \ (s_m, t_i \in D).$$

همهٔ t_i هاصفرنیستند (در غیر اینصورت ، $y_{m-1} - s_my_m = 0$ ، که با استقلال Y متناقض است) . هرگاه t_j اولین t_i ناصفر باشد ، آنگاه x_j ترکیبی خطی از y_{m-1} ، y_m ، وآن x_i هایی است که $i \neq j,k$. درنتیجه ، مجموعهٔ $\{x_i \mid i \neq j,k\} \cup \{y_{m-1}, y_m\}$ ، V رامی‌پیماید (زیرا X' چنین می‌کند) . بخصوص ، y_{m-2} ترکیبی خطی از y_{m-1} ، y_m ، و x_i به‌ازای $i \neq j,k$ است . بنابراین ، ممکن است فرایند افزودن یک y و حذف یک x فوق تکرار شود . در پایان مرحلهٔ k ام مجموعه‌ای خواهیم داشت مرکب از $y_m, y_{m-1}, \ldots, y_{m-k+1}$ و $n - k$ تا x_i که V را می‌پیماید . هرگاه $n < m$ ، آنگاه در پایان n مرحله نتیجه می‌شود که $\{y_m, \ldots, y_{m-n+1}\}$ ، V را می‌پیماید . چون $m - n + 1 \geq 2$ ، y_1 ترکیبی خطی از $y_m, \ldots, y_{m-n+1}$ است که استقلال خطی Y را نقض می‌کند . بنابراین ، باید داشته باشیم $m \leq n$. استدلالی مشابه ،که درآن نقشهای X و Y با هم عوض شده‌اند ، نشان می‌دهد که $n \leq m$ ؛ و لذا ؛ $m = n$.

تعریف ۸۰۲ . فرض کنیم R حلقه‌ای یکدار باشد به‌طوری‌که ، به‌ازای هر R ــ مدول F ، هر دو پایهٔ F دارای یک اصلیت باشند . در این صورت ، گوییم R دارای ***خاصیت بعد پایا*** است و عدد اصلی هر پایهٔ F **بعد** (یا **رتبهٔ**) F روی R نام دارد .

قضیهٔ ۷۰۲ می‌گوید که هر حلقهٔ بخشی دارای خاصیت بعد پایاست . ما از "بعد" در رابطه‌با فضاهای برداری روی یک حلقه بخشی و "رتبه" در رابطه با مدولهای آزاد روی حلقه‌های دیگر استفاده‌ای گسترده (ولی نه عام) خواهیم کرد . در اینجا بعد فضای برداری V روی‌حلقهٔ‌بخشی D را با $\dim_D V$ نشان‌می‌دهیم . خواص $\dim_D V$ بعد از نتیجهٔ ۱۲۰۲ بررسی خواهند شد . نتایج ۹۰۲ تا ۱۲۰۲ درآینده ، جز در بخشهای IV ۶۰ و VII ۵۰ ، لازم نمی‌شوند .

حکم ۹۰۲ . فرض کنیم E و F مدولهای آزادی روی حلقهٔ R باشند که از خاصیت بعد پایا برخوردارند . در این صورت ، $E \cong F$ اگر و فقط اگر E و F رتبه‌های یکسان داشته باشند .

برهان . تمرین ؛ ر.ک. حکم II ۳۰۱۰ .

لم ۱۰۰۲ . فرض کنیم R حلقه‌ای یکدار ، $I(\neq R)$ یک ایده‌آل F ، R یک R ــ مدول به پایهٔ X ، و $\pi : F \to F/IF$ برورپختی کانونی باشد . در این صورت ، F/IF یک R/I ــ مدول آزاد به پایهٔ $\pi(X)$ بوده و $|\pi(X)| = |X|$.

به یاد آورید که $IF = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in I,\ a_i \in F,\ n \in \mathbf{N}^* \right\}$ و عمل R/I بر F/IF با $(r + I)(a + IF) = ra + IF$ تعریف شده است (تمرین ۳۰۱) .

برهان ۱۰۰۲ . هرگاه $u + IF \in F/IF$ ، آنگاه $u = \sum_{j=1}^{n} r_j x_j$ که در آن $r_i \in R,\ x_i \in X$ ، زیرا $u \in F$ و X پایه‌ای از F است . درنتیجه ،

$$u + IF = (\sum_j r_i x_i) + IF = \sum_j (r_i x_i + IF) = \sum_j (r_i + I)(x_i + IF) = \sum_j (r_i + I)\pi(x_i),$$

که از آنجا $\pi(X)$ ، F/IF را به عنوان یک R/I ــ مدول تولید می‌کند . از طرف دیگر ، هرگاه $\sum_{k=1}^{m} (r_k + I)\pi(x_k) = 0$ که در آن $r_k \in R$ و $x_1, \ldots, x_m$ عناصر متمایزی از X اند ، آنگاه

$$0 = \sum_k (r_k + I)\pi(x_k) = \sum_k (r_k + I)(x_k + IF) = \sum_k r_k x_k + IF,$$

که از آنجا $\sum_k r_k x_k \in IF$. لذا ، $\sum_k r_k x_k = \sum_i s_i u_i$ ، که در آن $s_i \in I,\ u_i \in F$. چون هر u_i ترکیبی خطی از عناصر X بوده و I ایده‌آل است ، $\sum_j s_j u_j$ ترکیبی خطی از عناصر X با ضرایب در I می‌باشد . درنتیجه ، $\sum_{k=1} r_k x_k = \sum_j s_j u_j = \sum_{t=1}^{d} c_t y_t$ ، که در آنها

$c_i \in I$, $y_i \in X$. استقلال خطی X ایجاب می‌کند که (پس از اندیسگذاری مجدد و درج جملات $0x_k$, $0y_i$ در صورت لزوم) $m = d$ و، به‌ازای هر k، $x_k = y_k$ و $r_k = c_k \in I$. از اینرو، به‌ازای هر k، در R/I داریم $r_k + I = 0$ و $\pi(X)$ روی R/I مستقل خطی است. لذا، F/IF یک R/I ــ مدول‌به‌پایهٔ $\pi(X)$ است (قضیهٔ ۱۰۲) . بالاخره، هرگاه $x, x' \in X$ و، در F/IF، $\pi(x) = \pi(x')$، آنگاه $(1_R + I)\pi(x) - (1_R + I)\pi(x') = 0$. اگر $x \neq x'$ استدلال قبلی ایجاب می‌کند که $1_R \in I$، که با $I \neq R$ متناقض است. بنابراین، $x = x'$ و نگاشت $\pi : X \to \pi(X)$ یک بیژکسیون است؛ درنتیجه، $|X| = |\pi(X)|$.

حکم ۱۱۰۲ . *فرض کنیم $f : R \to S$ یک برووریختی ناصفراز حلقه‌های یکدار باشد. هرگاه S دارای خاصیت بعد پایا باشد، آنگاه R نیز این خاصیت را دارد.*

برهان. فرض کنیم $I = \operatorname{Ker} f$؛ پس $S \cong R/I$ (نتیجهٔ III ۱۰۲۰۲) . فرض کنیم X و Y پایه‌هایی از R ــ مدول F بوده و $\pi : F \to F/IF$ برووریختی کانونی باشد. بنابر لم ۱۰۲، F/IF یک R/I ــ مدول آزاد (و درنتیجه، یک S ــ مدول آزاد) با پایه‌های $\pi(X)$ و $\pi(Y)$ است به‌طوری که $|X| = |\pi(X)|, |Y| = |\pi(Y)|$. چون S دارای خاصیت بعد پایاست، $|\pi(X)| = |\pi(Y)|$. بنابراین، $|X| = |Y|$ و R دارای خاصیت بعد پایا می‌باشد.

نتیجهٔ ۱۲۰۲ . *هرگاه نقش همریختی از حلقهٔ یکدار R حلقه‌ای بخشی باشد، آنگاه R دارای خاصیت بعد پایاست. بخصوص، هر حلقهٔ تعویضپذیر یکدار از خاصیت بعد پایا برخوردار است.*

برهان. حکم اول از قضیهٔ ۷۰۲.۲ و حکم ۱۱۰۲ نتیجه می‌شود. هرگاه R تعویضپذیر و یکدار باشد، آنگاه R دارای ایده‌آل ماکزیمالی چون M (قضیهٔ III ۱۸۰۲۰) است و R/M میدان می‌باشد (قضیهٔ III ۲۰۰۲۰) . لذا، حکم دوم حالت خاصی از حکم اول می‌باشد.

حال به فضاهای برداری روی یک حلقهٔ بخشی بازگشته و خواص بعد را بررسی می‌کنیم. فضای‌برداری V روی‌حلقهٔ‌بخشی D را ***با بعد متناهی*** گویند اگر $\dim_D V$ متناهی

باشد.

قضیهٔ ۱۳۰۲ . فرض کنیم W زیرفضایی از فضای برداری V روی حلقهٔ بخشی D باشد .

(یک) $dim_D W \leq dim_D V$ ؛

(دو) هرگاه $dim_D W = dim_D V$ و $dim_D V$ متناهی باشد ، آنگاه $W = V$ ؛

(سه) $dim_D V = dim_D W + dim_D(V/W)$.

طرح برهان . (یک) فرض کنیم Y پایه‌ای از W باشد . بنابر قضیهٔ ۴۰۲ ، پایه‌ای مانند X از V شامل Y وجوددارد . بنابراین ، $\dim_D W = |Y| \leq |X| = \dim_D V$. (دو) هرگاه $|X| = |Y|$ و $|X|$ متناهی باشد ، آنگاه چون $Y \subset X$ ، باید داشته باشیم $Y = X$ ، که‌از آنجا $W = V$. (سه) نشان خواهیم داد که $U = \{x + W \mid x \in X - Y\}$ پایه‌ای از V/W است . این (طبق تعریف ۳۰۸ از آشنایی) ایجاب می‌کند که

$$\dim_D V = |X| = |Y| + |X - Y| = |Y| + |U| = \dim_D W + \dim_D(V/W).$$

هرگاه $v \in V$ ، آنگاه $v = \sum_i r_i y_i + \sum_j s_j x_j$ $(r_i, s_i \in D;\ y_i \in Y; x_j \in X - Y)$ ؛ درنتیجه ،

$v + W = \sum_j s_j(x_j + W)$. بنابراین ، U ، V/W را می‌پیماید . هرگاه

$\sum_j r_j(x_j + W) = 0\,(r_j \in D; x_j \in X - Y)$ ، آنگاه $\sum_j r_j x_j \in W$ ، که از آنجا

$\sum_j r_j x_j = \sum_k s_k y_k$ $(s_k \in D; y_k \in Y)$. این استقلال خطی $X = Y \cup (X - Y)$ را نقض می‌کند مگر آنکه به‌ازای هر j,k ، $r_j = 0, s_k = 0$. بنابراین ، U مستقل خطی بوده و $|U| = |X - Y|$.

نتیجهٔ ۱۴۰۲ . هرگاه $f : V \to V'$ تبدیلی خطی از فضاهای برداری روی حلقهٔ بخشی D باشد ، آنگاه پایه‌ای از V مانند X وجود دارد به‌طوری‌که $X \cap Ker\, f$ پایه‌ای از $Ker\, f$ بوده و $\{f(x) \mid f(x) \neq 0, x \in X\}$ پایه‌ای از $Im\, f$ می‌باشد . بخصوص ،

$$dim_D V = dim_D(Ker\, f) + dim_D(Im\, f).$$

طرح برهان. برای اثبات حکم اول، فرض کنیم $W = \mathrm{Ker}\, f$ و Y, X همانند در برهان قضیهٔ ۱۳۰۲ باشد. حکم دوم از قضیهٔ ۱۳۰۲ (سه) نتیجه می‌شود، زیرا، طبق قضیهٔ ۷۰۱، $V/W \cong \mathrm{Im}\, f$.

نتیجهٔ ۱۵۰۲. *هرگاه V و W زیرفضاهایی با بعد متناهی از یک فضای برداری روی حلقهٔ بخشی D باشد، آنگاه*

$$dim_D V + dim_D W = dim_D(V \cap W) + dim_D(V + W).$$

طرح برهان. فرض کنیم X پایه‌ای از $V \cap W$، Y پایه‌ای (متناهی) از V شامل X، و Z پایه‌ای (متناهی) از W باشد که شامل X است (قضیهٔ ۴۰۲). نشان دهید که $X \cup (Y - X) \cup (Z - X)$ پایه‌ای از $V + W$ می‌باشد، که از آنجا

$$\begin{aligned}\dim_D(V + W) = |X| + |Y - X| + |Z - X| &= \dim_D(V \cap W) \\ &+ (\dim_D V - \dim_D(V \cap W)) \\ &+ (\dim_D W - \dim_D(V \cap W)).\end{aligned}$$

به یاد آورید که هرگاه حلقهٔ بخشی R مشمول حلقهٔ بخشی S باشد، آنگاه S یک فضای‌برداری روی R است که در آن rs $(s \in S, r \in R)$ حاصل‌ضرب معمولی در S می‌باشد. قضیهٔ زیر برای مطالعهٔ توسیعهای میدان در فصل پنج لازم خواهد شد.

قضیهٔ ۱۶۰۲. *فرض کنیم R, S, T حلقه‌هایی بخشی باشند به‌طوری‌که $R \subset S \subset T$. در این صورت،*

$$dim_R T = (dim_S T)(dim_R S).$$

به علاوه، $dim_R T$ متناهی است اگر و فقط اگر $dim_S T$ و $dim_R S$ متناهی باشند.

برهان. فرض کنیم U پایه‌ای از T روی S بوده، و V پایه‌ای از S روی R باشد. کافی است نشان دهیم که $\{vu \mid v \in V, u \in U\}$ پایه‌ای از T روی R است. بنابر استقلال خطی U روی S، عناصر vu همه متمایزند. درنتیجه، می‌توان نتیجه گرفت که $\dim_R T = |U||V| = (\dim_S T)(\dim_R S)$. در این صورت، آخرین حکم قضیه فورا" نتیجه

می‌شود ، زیـرا حاصـل‌ضرب دو عدد اصلی متناهی متناهی است و حاصل‌ضرب یک عدد اصلی نامتناهی در یک عـدد اصلی متناهی نامتناهی می‌باشد (آشنایی، قضیهٔ ۱۱۰۸) .

هرگاه $u \in T$ ، آنگاه $u = \sum_{i=1}^{n} s_i u_i \ (s_i \in S, u_i \in U)$ ، زیرا T ، U رابه‌عنوان یک فضای برداری روی S می‌پیماید . چون S یک فضای برداری روی R است ، هر s_i را می‌توان به صورت $s_i = \sum_{j=1}^{m_j} r_{ij} v_j \ (r_{ij} \in R, v_j \in V)$ نوشت . لذا ، $u = \sum_i s_i u_i = \sum_i (\sum_j r_{ij} v_j) u_i = \sum_i \sum_j r_{ij} v_j u_i$. بنابراین ، T ، $\{vu | v \in V, u \in U\}$ را بـه عنوان یک فضای برداری روی R می‌پیماید .

فـرض کنیـم $\sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij}(v_j u_i) = 0 \quad (r_{ij} \in R, v_j \in V, u_i \in U)$. بـه‌ازای هـر i ، قرار می‌دهیم $s_i = \sum_{j=1}^{m} r_{ij} v_j \in S$. دراین‌صورت ، $0 = \sum_i \sum_j r_{ij}(v_j u_i) = \sum_i (\sum_j r_{ij} v_j) u_i = \sum_i s_i u_i$. استقلال خطی U روی S ایجاب می‌کند که به‌ازای هر i ، $0 = s_i = \sum_j r_{ij} v_j$. استقلال خطی V روی R ایجاب می‌کند که به‌ازای هر i,j ، $r_{ij} = 0$. بنابراین ، $\{vu \mid v \in V, u \in U\}$ روی R مستقل خطی است ، و درنتیجه ، یک پایه می‌باشد .

تمرینات

۱ . (آ) مجموعهٔ $\{x_1, \ldots, x_n\}$ از بردارها در فضای برداری V روی حلقهٔ بخشی R وابستهٔ خطی است اگر و فقط اگر x_k ای ترکیب خطی x_i های پیش از آن بـاشد .
(ب) هرگاه $\{x_1, x_2, x_3\}$ یک زیرمجموعهٔ مستقل خطی از V باشد ، آنگاه مجموعهٔ $\{x_1 + x_2,\ x_2 + x_3,\ x_3 + x_1\}$ مستقل خطـی است اگر و فقط اگر $\text{Char } R \neq 2$ [ر.ک. تعریف III ۸۰۱۰] .

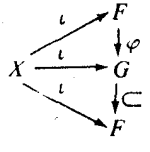
۲ . فرض کنید R حلقه‌ای (احتمالاً بدون واحد) بوده و X مجموعه‌ای ناتهی باشد . در این تمرین ، R ــ مدول F یک **مدول آزاد بر X** نامیده می‌شود اگر F یک شیٔ آزادبر X در رستهٔ تمام R ــ مدولها باشد . لذا ، طبق تعریف ۷۰۷۰ ، F یک مدول آزاد بر X است اگر تابعی مانند $\iota : X \to F$ موجود باشد به‌طوری‌که به‌ازای هر R ــ مدول A و تابع $f : X \to A$ ، همریختی منحصر به فردی از R ــ مدولها مانند $\bar{f} : F \to A$ موجود باشد که $\bar{f}\iota = f$.

(آ) فرض کنید $\{X_i \mid i \in I\}$ گردایه‌ای از مجموعه‌های دو به دو از هم جدا بوده و به‌ازای هر $i \in I$ ، F_i یک مدول آزاد بر X_i باشد که $\iota_i : X_i \to F_i$. فرض کنید $X = \bigcup_{i \in I} X_i$ و $F = \sum_{i \in I} F_i$ ، که در آن $\phi_i : F_i \to F$ انژکسیون کانونی است. $\iota : X \to F$ را به‌ازای $x \in X_i$ با $\iota(x) = \phi_i \iota_i(x)$ تعریف کنید (i تعریف شده‌است، زیرا X_i ها ازهم جدایند) . ثابت کنید F یک مدول آزاد بر X است. [**راهنمایی .** قضیهٔ ۱۳۰۱ ممکن است مفید باشد .]

(ب) فرض کنید R یکدار باشد. همچنین، به گروه آبلی $\mathbf{Z}$ ساختار R ــ مدول بدیهی داده شده باشد (به‌ازای هر $r \in R, m \in \mathbf{Z}$ ، $rm = 0$) ؛ درنتیجه، $R \oplus \mathbf{Z}$ یک R ــ مدول است که در آن به‌ازای هر $r,r' \in R, m \in \mathbf{Z}$ ، $r(r',m) = (rr',0)$. اگر X یک مجموعهٔ تک‌عنصری باشد ، مثلاً $X = \{t\}$ ، فرض کنیم تابع $\iota : X \to R \oplus \mathbf{Z}$ با $\iota(t) = (1_R,1)$ داده شده باشد. ثابت کنید $R \oplus \mathbf{Z}$ یک مدول آزاد بر X است. [**راهنمایی .** اگر $f : X \to A$ ، مثل تمرین ۱۷۰۱ قرار دهید $A = B \oplus C$ ؛ درنتیجه، $f(t) = b + c$ ($b \in B, c \in C$) . تعریف کنید $f(r,m) = rb + mc$.]

(پ) هرگاه R یک حلقهٔ دلخواه بوده و X یک مجموعه باشد ، آنگاه یک مدول آزاد بر X وجوددارد . [**راهنمایی .** چون X اجتماع‌ازهم‌جدایی‌از مجموعه‌های $\{t\}$ که $t \in X$ می‌باشد ، بنابر (آ) کافی است فرض کنید X فقط یک عنصر دارد . اگر R یکدار باشد ، از (ب) استفاده کنید . اگر R یکدار نباشد ، R را در حلقهٔ یکدار S با مشخص 0 ، مثل برهان قضیهٔ III ۱۰۰۱۰ ، بنشانید . با استفاده از تمرین ۱۸۰۱ ، نشان دهید که S یک R ــ مدول آزاد بر X است .]

۳ . فرض کنید R یک حلقه (احتمالاً بدون واحد) بوده و F یک R ــ مدول آزاد بر مجموعهٔ X باشد که ، مثل تمرین ۲ ، $\iota : X \to F$. نشان دهید که $\iota(X)$ مجموعهٔ مولدهای R ــ مدول F است . [**راهنمایی .** فرض کنید G زیرمدول F تولید شده با $\iota(X)$ بوده و ، با استفاده از تعریف "مدول آزاد" ، نشان دهید که یک همریختی مدولها مانند φ وجود دارد به‌طوری‌که



تعویضپذیر است. نتیجه بگیرید که $\varphi = 1_F$.]

۴. فرض کنید R یک دامنهٔ ایده‌آل اصلی، A یک R ــ مدول چپ یکانی، و $p \in R$ اول (≠تحویل‌ناپذیر) باشد. قرار دهید $pA = \{pa \mid a \in A\}$ و $A[p] = \{a \in A \mid pa = 0\}$.

(آ) $R/(p)$ یک میدان است (قضایای III ۲۰.۲۰ و III ۴.۳۰).

(ب) pA و $A[p]$ زیرمدولهایی از A هستند.

(پ) A/pA یک فضای برداری روی $R/(p)$ است، که در آن $(r + (p))(a + pA) = ra + pA$.

(ت) $A[p]$ یک فضای برداری روی $R/(p)$ است، که در آن $(r + (p))a = ra$.

۵. فرض کنید V یک فضای برداری روی حلقهٔ بخشی D بوده و S مجموعهٔ تمام زیرفضاهای V باشد که با شمول نظریهٔ مجموعه‌ها جزئی مرتب شده است.

(آ) S یک شبکهٔ تام است (ر.ک. آشنایی، تمرین ۲.۷؛ کوچکترین کران بالایی V_1, V_2 مساوی $V_1 + V_2$ و بزرگترین کران پایینی آن $V_1 \cap V_2$ است).

(ب) S یک شبکهٔ مکمل است؛ یعنی، به‌ازای هر $V_1 \in S$، $V_2 \in S$ ای وجود دارد به‌طوری‌که $V = V_1 + V_2$ و $V_1 \cap V_2 = 0$؛ درنتیجه، $V = V_1 \oplus V_2$.

(پ) S یک شبکهٔ مدولی است؛ یعنی، هرگاه $V_1, V_2, V_3 \in S$ و $V_3 \subset V_1$، آنگاه
$$V_1 \cap (V_2 + V_3) = (V_1 \cap V_2) + V_3.$$

۶. فرض کنید $\mathbf{R}$ و $\mathbf{C}$ به ترتیب میدان اعداد حقیقی و مختلط باشند.

(آ) $\dim_{\mathbf{R}} \mathbf{C} = 2$ و $\dim_{\mathbf{R}} \mathbf{R} = 1$.

(ب) میدانی مانند K که $\mathbf{R} \subset K \subset \mathbf{C}$ وجود ندارد.

۷. هرگاه گروه نابدیهی G دوری از مرتبهٔ 2 نباشد، آنگاه G دارای یک خودریختی غیرهمانی است. **[راهنمایی.** تمرین II ۱۱.۴۰ و تمرین ۴ (ت) فوق.]

۸. هرگاه V یک فضای برداری با بعد متناهی بوده و V^m فضای برداری
$$V \oplus V \oplus \cdots \oplus V \quad (m \text{ جمعوند})$$
باشد آنگاه، به‌ازای هر $m \geq 1$، V^m با بعدمتناهی است و $\dim V^m = m(\dim V)$.

۹. هرگاه F_1 و F_2 مدولهای آزادی‌روی یک حلقهٔ دارای خاصیت بعد پایا باشد، آنگاه $\operatorname{rank}(F_1 \oplus F_2) = \operatorname{rank} F_1 + \operatorname{rank} F_2$.

۱۰. فرض کنید R یک حلقهٔ بدون مقسوم علیه صفر باشد به‌طوری که به‌ازای هر $r, s \in R$، $a, b \in R$ ای که هر دو صفر نیستند وجود دارند که $ar + bs = 0$.

(آ) هرگاه $R = K \oplus L$ (مجموع مستقیم مدولها)، آنگاه $K = 0$ یا $L = 0$.
(ب) هرگاه R یکدار باشد، آنگاه R دارای خاصیت بعد پایاست.

۱۱. فرض کنید F یک مدول آزاد با رتبهٔ نامتناهی α روی حلقهٔ باشد که دارای خاصیت بعد پایاست. به‌ازای هر عدد اصلی β که $0 \leq \beta \leq \alpha$، F دارای بی‌نهایت زیرمدول آزاد حقیقی با رتبهٔ β است.

۱۲. هرگاه F یک مدول آزاد روی حلقه‌ای یکدار بوده به‌طوری‌که F دارای پایه‌ای به اصلیت متناهی $n \geq 1$ و پایهٔ دیگری به اصلیت $n+1$ باشد، آنگاه F دارای پایه‌ای به اصلیت m، به‌ازای هر $m \geq n$ $(m \in \mathbf{N}^*)$، خواهد بود.

۱۳. فرض کنید K حلقه‌ای یکدار بوده و F یک K ــ مدول با پایهٔ شمارشپذیر نامتناهی $\{e_1, e_2, \ldots\}$ باشد. طبق تمرین ۷۰۱ (ب)، $R = \mathrm{Hom}_K(F,F)$ یک حلقه است. هرگاه n عدد صحیح مثبتی باشد، آنگاه R ــ مدول چپ آزاد R دارای پایه‌ای از n عنصر است؛ یعنی، به عنوان یک R ــ مدول، به‌ازای هر تعداد جمعوند، $R \cong R \oplus \cdots \oplus R$. [**راهنمایی.** $\{1_R\}$ یک پایهٔ تک عنصری است؛ $\{f_1, f_2\}$ یک پایهٔ دو عنصری است، که در آن $f_1(e_{2n}) = e_n$، $f_1(e_{2n-1}) = 0$، $f_2(e_{2n}) = 0$، و $f_2(e_{2n-1}) = e_n$. توجه کنید که به‌ازای هر $g \in R$، $g = g_1 f_1 + g_2 f_2$، که در آن $g_1(e_n) = g(e_{2n})$ و $g_2(e_n) = g(e_{2n-1})$.]

۱۴. فرض کنید $f : V \to V'$ یک تبدیل‌خطی از فضاهای برداری با بعد متناهی V و V' باشد به‌طوری‌که $\dim V = \dim V'$. در این صورت، شرایط زیر باهم معادلند: (یک) f یکریختی‌است؛ (دو) f بروریختی‌است؛ (سه) f تکریختی است. [**راهنمایی.** نتیجهٔ ۱۴۰۲.]

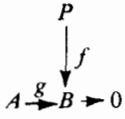
۱۵. فرض کنید R یک حلقهٔ یکدار باشد. نشان دهید که R یک مدول آزاد روی یک مجموعه در رستهٔ **تمام** R ــ مدولها (به صورت تعریف شده در تمرین ۲) **نیست.** [**راهنمایی.** گروه‌آبلی‌ناصفر A را با ساختار R ــ مدول بدیهی ($ra = 0$ به‌ازای هر $r \in R, a \in A$) درنظر بگیرید. توجه کنید که تنها همریختی $R \to A$ از مدولها نگاشت صفر است.]

۳ مدولهای تصویری و انژکتیو

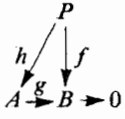
هر مدول‌آزاد تصویری است و مدولهای تصویری دلخواه (که لزوما "آزاد نیستند) بعضی

از خواص مدولهای آزاد را دارند . مدولهای تصویری بویژه در محدودهٔ رسته‌ها مفیدند ، زیرا صرفا" برحسب مدولها و همریختیها تعریف شده‌اند . انژکتیوی ، که در اینجا نیز مطالعه شده است ، مفهوم دوگان تصویری است .

تعریف ۱۰۳ . گوییم مدول P روی حلقهٔ R **تصویری** است اگر به‌ازای هر نمودار

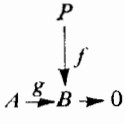


از همریختیهای R ــ مدولها که سطر پایین آن کامل باشد (یعنی ، g برو ریختی باشد) یک همریختی R ــ مدولها مانند $h : P \to A$ وجود داشته باشد به‌طوری که نمودار

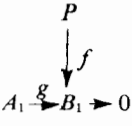


تعویضپذیر باشد (یعنی ، $gh = f$) .

قضایای زیر چند مثال از مدولهای تصویری است . ابتدا توجه می‌کنیم که هرگاه R یکدار بوده و P یکانی باشد ، آنگاه P تصویری است اگر و فقط اگر به‌ازای هر جفت مدول **یکانی** مانند A, B و نمودار



ازهمریختیهای R ــ مدولهاکه در آن g بروریختی است ، یک همریختی مانند $h : P \to A$ وجودداشته‌باشد که $gh = f$. زیرا ، طبق تمرین ۱۷۰۱ ، $A = A_1 \oplus A_2$ و $B = B_1 \oplus B_2$ که در آنها A_1 و B_1 یکانی بوده و $RA_2 = 0 = RB_2$. تمرین ۱۷۰۱ نشان می‌دهد که $f(P) \subset B_1$ و $g \mid A_1$ یک بروریختی $A_1 \to B_1$ است ؛ درنتیجه ، نمودار



از مدولهای یکانی را خواهیم داشت. لذا، وجود $h : P \to A$ که $gh = f$ معادل وجود $h : P \to A_1$ که $gh = f$ می‌باشد.

قضیهٔ ۲۰۳ . هر مدول آزاد F روی حلقهٔ یکدار R تصویری است.

تبصره. قضیه در صورتی که عبارت "یکدار بودن" حذف شده و F یک مدول آزاد در رستهٔ تمام R ــ مدولهای چپ (به صورت تعریف شده در تمرین ۲۰۲) باشد نیز درست است. برهان زیر کلمه به کلمه قابل ذکر است، مشروط بر اینکه به جای قضیهٔ ۱۰۲ از تمرین ۲۰۲ استفاده کرده و کلمهٔ "یکانی" حذف گردد.

برهان ۲۰۳ . در پرتو تبصره‌های پیش از قضیه، می‌توان فرض کرد نمودار

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow f & & \\ A & \xrightarrow{g} & B & \to & 0 \end{array}$$

از همریختیهای R ــ مدولهای یکانی داده شده باشد، که در آن g یک بروریختی بوده و F یک R ــ مدول آزاد برمجموعهٔ X است $(\iota : X \to F)$. به‌ازای هر $x \in X$ ، $f(\iota(x)) \in B$. چون g بروریختی است، $a_x \in A$ ی هست که $g(a_x) = f(\iota(x))$. چون F آزاد است، نگاشت $X \to A$ داده‌شده با $x \mapsto a_x$ یک همریختی از R ــ مدولها مانند $h : F \to A$ را القا می‌کند به‌طوری که به‌ازای هر $x \in X$ ، $h(\iota(x)) = a_x$. در نتیجه، به‌ازای هر $x \in X$ ، $ghi(x) = g(a_x) = fi(x)$ ؛ لذا، $gh\iota = f\iota : X \to B$. طبق قسمت یکتایی قضیهٔ ۱۰۲ (چهار)، داریم $gh = f$. بنابراین، F تصویری می‌باشد.

نتیجهٔ ۳۰۳ . هر مدول A روی حلقهٔ R نقش همریخت یک R ــ مدول تصویری است.

برهان. این نتیجه فورا" از قضیهٔ ۲۰۳ و نتیجهٔ ۲۰۲ به دست می‌آید.

قضیهٔ ۴۰۳ . فرض کنیم R یک‌حلقه باشد. شرایط زیر بر R ــ مدول P باهم معادلند:
(یک) P تصویری است؛

(دو) *هر دنبالهٔ کامل کوتاه* $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ *کامل تجزیه است (از اینرو،* $B \cong A \oplus P$*)؛*

(سه) *مدول آزاد* F *و* R *ـ مدول* K *وجود دارند به‌طوری‌که* $F \cong K \oplus P$.

تبصره. عبارت "مدول آزاد" در شرط (سه) را می‌توان در صورتی که R یکدار بوده و P یکانی باشد به معنی قضیهٔ ۱۰۲ و، در غیر این صورت، به معنی تمرین ۲۰۲ تعبیر کرد. برهان در هر حالت یکی است.

برهان ۴۰۳. (دو) $\Rightarrow$ (یک) نمودار

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle 1_P} & & \\ B & \xrightarrow{g} & P & \to & 0 \end{array}$$

با سطر پایین کامل را طبق فرض درنظر می‌گیریم. چون P تصویری است، یک همریختی R ـ مدولها مانند $h : P \to B$ وجود دارد به‌طوری‌که $gh = 1_P$. بنابراین، دنبالهٔ کامل کوتاه $0 \to A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} P \to 0$، طبق قضیهٔ ۱۸۰۱، کامل تجزیه است و $B \cong A \oplus P$.

(سه) $\Rightarrow$ (دو) طبق نتیجهٔ ۲۰۲، R ـ مدول آزاد F و بروریختی $g : F \to P$ وجود دارند. هرگاه $K = \operatorname{Ker} g$، آنگاه $0 \to K \xrightarrow{\subseteq} F \xrightarrow{g} P \to 0$ کامل است. طبق فرض، دنباله تجزیه شده است؛ درنتیجه، طبق قضیهٔ ۱۸۰۱، $F \cong K \oplus P$.

(یک) $\Rightarrow$ (سه) فرض کنیم π ترکیب $F \cong K \oplus P \to P$ باشد، که در آن نگاشت دوم تصویر کانونی است. به همین نحو، فرض کنیم ι ترکیب $P \to K \oplus P \cong F$ باشد که در آن اولین نگاشت انژکسیون کانونی است. با داشتن نمودار

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \to & 0 \end{array}$$

از همریختیهای R ـ مدولها که سطر پایین آن کامل است، نمودار

$$\begin{array}{ccccc} & & F & & \\ & & \pi \downarrow \uparrow \iota & & \\ & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \to & 0 \end{array}$$

را درنظر می‌گیریم . چون F طبق قضیهٔ ۲.۳ تصویری است ، یک همریختی R ــ مدولها مانند $h_1 : F \to A$ وجود دارد به‌طوری‌که $gh_1 = f\pi$. فرض کنیم $h = h_1\iota : P \to A$. در این صورت ،

$$gh = gh_1\iota = (f\pi)\iota = f(\pi\iota) = f1_P = f.$$

بنابراین ، P تصویری است .

مثال . هرگاه $R = Z_6$ ، آنگاه Z_3 و Z_2 ، Z_6 ــ مدول بوده (ر.ک. تمرین ۱.۱) و یک یکریختی Z_6 ــ مدولها مانند $Z_6 \cong Z_2 \oplus Z_3$ وجود دارد . از اینرو ، Z_2 و Z_3 ، Z_6 ــ مدولهای تصویری‌اند که Z_6 ــ مدول آزاد نیستند .

حکم ۵.۳ . فرض کنیم R یک‌حلقه‌باشد . مجموع مستقیم $\sum_{i\in I} P_i$ از R ــ مدولها تصویری است اگر و فقط اگر هر P_i تصویری باشد .

طرح برهان . فرض کنیم $\sum P_i$ تصویری باشد . چون در برهان (یک) $\Rightarrow$ (سه) در قضیهٔ ۴.۳ فقط ازتصویری بودن F استفاده شده ، این برهان در صورت قرار $\sum_{i\in I} P_i$ ، $\sum_{i\neq j} P_i$ ، و P_j به‌جای K ، F ، و P معتبر می‌ماند . عکس مطلب با تکنیکهایی مشابه و با استفاده از نمودار

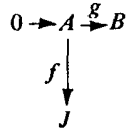
$$\begin{array}{ccc} & & P_j \\ & & \iota_j \downarrow\uparrow \pi_j \\ & & \sum P_i \\ & & \downarrow f \\ A & \xrightarrow{g} & B \longrightarrow 0 \end{array}$$

ثابت می‌شود . هرگاه هر P_i تصویری باشد ، آنگاه به‌ازای هر j ، $h_i : P_i \to A$ ای وجود دارد به‌طوری که $gh_i = f\iota_i$. بنابر قضیهٔ ۱۳.۱ ، همریختی منحصر به فردی مانند $h : \sum P_i \to A$ وجود دارد که به‌ازای هر j ، $h\iota_i = h_i$. تحقیق کنید که $gh = f$.

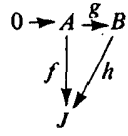
به یاد آورید که دوگان یک مفهوم تعریف شده در یک رسته (یعنی ، تعریف شده برحسب اشیاءوریختها) با "عکس کردن تمام سهمها" به دست می‌آید . این ایده را کمی

جلوتربرده‌ومی‌گوییم یک تکریختی دوگان یک بروریختی است ، زیرا $A \to B$ یک تکریختی است اگر و فقط اگر $0 \to A \to B$ کامل باشد و $B \to A$ یک بروریختی است اگر و فقط اگر $B \to A \to 0$ (سهمها عکس شده‌اند !) کامل باشد . این ما را به تعریف مفهوم‌دوگان تصویری به صورت زیر می‌کشاند .

تعریف ۶.۳ . گوییم مدول J روی حلقهٔ R *انژکتیو* است اگر به‌ازای هر نمودار



از همریختیهای R ــ مدولها باسطر بالای کامل (یعنی ، g یک‌تکریختی) ،یک همریختی‌از R ــ مدولها مانند $h : B \to J$ وجود داشته باشد به‌طوری‌که نمودار



تعویضپذیر باشد (یعنی ، $hg = f$) .

نکاتی شبیه آنچه‌دربند بعد از تعریف ۱.۳ آمد را می‌توان در اینجا برای مدولهای انژکتیویکانی‌روی یک حلقهٔ یکدار بیان کرد . اینکه دوگان بسیاری (ولی نه همهٔ) احکام پیش را می‌توان به آسانی ثابت کرد تعجب‌آور نیست . مثلا " ، چون در یک رسته حاصل‌ضربها مفهوم دوگان هم‌حاصل‌ضربها (مجموعهای مستقیم) هستند ، دوگان حکم ۵.۳ عبارت است از

حکم ۷.۳ . *حاصل‌ضرب مستقیم* $\prod_{i \in I} J_i$ *از* R ــ *مدولها انژکتیواست اگر و فقط‌اگر* J_i ، *به‌ازای هر* $i \in I$ ، *انژکتیو باشد* .

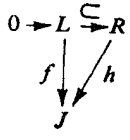
برهان . تمرین؛ ر.ک. حکم ۵.۳ .

چون مفهوم یک مدول آزاد قابل دوگان شدن نیست (تمرین ۱۳) ، مشابه‌های قضایای ۲.۳ یا ۴.۳ (سه) برای مدولهای انژکتیو وجود ندارند . اما نتیجهٔ ۳.۳ را

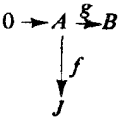
می‌توان دوگان ساخت. درواقع، می‌گوید که به‌ازای هر مدول A، یک مدول تصویری مانند P و یک دنباله‌ٔ کامل چون $P \to A \to 0$ وجود دارند. دوگان این حکم این است که به‌ازای هر مدول A، یک مدول انژکتیو مانند J و یک دنباله‌ٔ کامل چون $0 \to A \to J$ وجود دارند؛ به عبارت دیگر، هر مدول را می‌توان در یک مدول انژکتیو نشانید. باقیماندهٔ این بخش، که در آینده به کار نمی‌آید، به اثبات این امر برای مدولهای یکانی روی یک حلقهٔ یکدار اختصاص دارد. پس از این کار، اثبات دوگان قضایای ۴۰۳ (یک) و (دو) آسان است (حکم ۱۳۰۳). بحث را با توصیف R ــ مدولهای انژکتیو برحسب ایده‌آلهای چپ (زیرمدولهای) حلقهٔ R آغاز می‌کنیم.

لم ۸۰۳. *فرض کنیم R حلقه‌ای یکدار باشد. R ــ مدول یکانی J انژکتیو است اگر و فقط اگر به‌ازای هر ایده‌آل چپ L از R، هر همریختی $L \to J$ از R ــ مدولها را بتوان به یک همریختی $R \to J$ از R ــ مدولها توسیع داد.*

طرح برهان. منظور از توسیع $f : L \to J$ به R یعنی یک همریختی مانند $h : R \to J$ وجود دارد به‌طوری‌که نمودار



تعویض‌پذیر است. واضح است که اگر J انژکتیو باشد، h همواره وجود دارد. به عکس، فرض کنیم J دارای خاصیت توسیع ذکر شده بوده و نمودار



از همریختیهای مدولها که سطر بالایی آن کامل است موجود باشد. برای آنکه نشان دهیم J انژکتیو است، باید یک همریختی $h : B \to J$ با خاصیت $hg = f$ را بیابیم. فرض کنیم $\mathcal{S}$ مجموعهٔ تمام همریختیها مانند $h : C \to J$ از R ــ مدولها باشد، که $\operatorname{Im} g \subset C \subset B$. $\mathcal{S}$ ناتهی است، زیرا $fg^{-1} : \operatorname{Im} g \to J$ عنصری از $\mathcal{S}$ است (g یک تکریختی است). $\mathcal{S}$

را با توسیع جزئی مرتب می‌کنیم: $h_1 \leq h_2$ اگر و فقط اگر $\mathrm{Dom}\, h_1 \subset \mathrm{Dom}\, h_2$ و $h_2 \mid \mathrm{Dom}\, h_1 = h_1$. تحقیق کنیدکه مفروضات لم زرن برقرارند و نتیجه بگیرید که $\mathcal{S}$ شامل عنصر ماکزیمالی چون $h : H \to J$ است که $hg = f$. برهان را با اثبات $H = B$ کامل می‌کنیم.

هرگاه $H \neq B$ و $b \in B - H$، آنگاه $L = \{r \in R \mid rb \in H\}$ یک‌ایده‌آل‌چپ R است. نگاشت $L \to J$ داده شده با $r \mapsto h(rb)$ یک همریختی R ــ مدولهای تعریف شده است. طبق فرض، یک همریختی R ــ مدولها مانند $k : R \to J$ وجود دارد به‌طوری‌که به‌ازای هر $r \in L$، $k(r) = h(rb)$. فرض کنید $c = k(1_R)$ و نگاشت $\bar{h} : H + Rb \to J$ را با تعریف می‌کنیم $a + rb \mapsto h(a) + rc$. حکم می‌کنیم که $\bar{h}$ تعریف شده است. زیرا هرگاه $a_1 + r_1 b = a_2 + r_2 b \in H + Rb$، آنگاه $a_1 - a_2 = (r_2 - r_1)b \in H \cap Rb$. از اینرو، $r_2 - r_1 \in L$ و

$$h(a_1) - h(a_2) = h(a_1 - a_2) = h((r_2 - r_1)b) = k(r_2 - r_1) = (r_2 - r_1)k(1_R) = (r_2 - r_1)c.$$

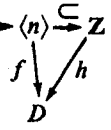
بنابراین، $\bar{h}(a_1 + r_1 b) = h(a_1) + r_1 c = h(a_2) + r_2 c = h(a_2 + r_2 b)$ و $\bar{h}$ تعریف شده است. تحقیق کنید که $\bar{h} : H + Rb \to J$ یک‌همریختی R ــ مدولهاوعنصری از مجموعهٔ $\mathcal{S}$ است. این باماکزیمالی h تعارض دارد، زیرا $b \notin H$؛ و درنتیجه، $H \subsetneq H + Rb$. بنابراین، $H = B$ و J انژکتیو است.

گوییم گروه آبلی D **بخشپذیر** است اگر به‌ازای هر $y \in D$ و $0 \neq n \in \mathbf{Z}$، $x \in D$ ی وجود داشته باشد به‌طوری که $nx = y$. مثلاً "، گروه جمعی $\mathbf{Q}$ بخشپذیر است، ولی $\mathbf{Z}$ نیست (تمرین ۴). به آسانی ثابت می‌شود که یک مجموع مستقیم از گروههای آبلی بخشپذیر است اگر و فقط اگر هر جمعوند بخشپذیر باشد، و نیز نقش همریخت یک گروه بخشپذیر بخشپذیر است (تمرین ۷).

لم ۹.۳. گروه آبلی D بخشپذیراست‌اگرو فقط‌اگر D یک $\mathbf{Z}$ ــ مدول (یکانی) انژکتیو باشد.

برهان. اگر D انژکتیو بوده، $y \in D$، و $0 \neq n \in \mathbf{Z}$، $f : \langle n \rangle \to D$ را همریختی منحصر به‌فردی می‌گیریم که با $n \mapsto y$ معین می‌شود؛ ($\langle n \rangle$، طبق قضیهٔ I ۲.۳۰ و II ۱.۱۰،

یک $\mathbf{Z}$ ـ مدول آزاد است) . چون D انژکتیو است، یک همریختی مانند $h : \mathbf{Z} \to D$ وجود دارد به‌طوری که نمودار



تعویضپذیر است. هرگاه $x = h(1)$ ، آنگاه $nx = nh(1) = h(n) = f(n) = y$. بنابراین، D بخشپذیر است. برای اثبات عکس، توجه کنید که تنها ایده‌آلهای چپ $\mathbf{Z}$ گروههای دوری $\langle n \rangle$ ، $n \in \mathbf{Z}$ ، هستند. هرگاه D بخشپذیر بوده و $f : \langle n \rangle \to D$ یک همریختی باشد، آنگاه $x \in D$ ی وجود دارد که $nx = f(n)$. $h : \mathbf{Z} \to D$ را با $1 \mapsto x$ تعریف کرده و تحقیق کنید h یک همریختی است که f را توسیع می‌دهد. بنابراین، طبق لم ۸۰۳ ، D انژکتیو است.

تبصره. توصیف کامل گروههای آبلی بخشپذیر ($\mathbf{Z}$ ـ مدولهای یکانی انژکتیو) در تمرین ۱۱ داده شده است.

لم ۱۰۰۳ . *هر گروه آبلی A را می‌توان در یک گروه آبلی بخشپذیر نشانید.*

برهان. بنابر قضیهٔ II ۴۰۱۰ ، یک $\mathbf{Z}$ ـ مدول آزاد مانند F و یک برووریختی چون $F \to A$ با هستهٔ K وجود دارند به‌طوری که $F/K \cong A$. چون F مجموع مستقیمی از نسخه‌های $\mathbf{Z}$ است (قضیهٔ II ۱۰۱۰) و $\mathbf{Z} \subset \mathbf{Q}$ ، F را می‌توان در مجموع مستقیم D از نسخه‌های اعداد گویای $\mathbf{Q}$ نشانید (قضیهٔ I ۱۰۰۸۰). اما، بنابر حکم ۷۰۳ ، لم ۹۰۳ ، و تبصره‌های پیش از آن، D یک گروه بخشپذیر است. هرگاه $f : F \to D$ تکریختی نشاننده باشد، آنگاه، طبق نتیجهٔ I ۸۰۵۰ ، F یک یکریختی $F/K \cong f(F)/f(K)$ را القا می‌کند لذا، ترکیب $A \cong F/K \cong f(F)/f(K) \subset D/f(K)$ یک تکریختی است. اما $D/f(K)$ بخشپذیر است، زیرا نقش همریخت یک گروه بخشپذیر می‌باشد.

هرگاه R حلقه‌ای یکدار بوده و J گروهی آبلی باشد، آنگاه $\mathbf{Hom}_{\mathbf{Z}}(R,J)$ ، یعنی مجموعهٔ تمام همریختیهای $R \to J$ از $\mathbf{Z}$ ـ مدولها یک گروه آبلی است (تمرین ۷۰۱) .

تحقیق کنید که $\mathrm{Hom}_{\mathbf{Z}}(R,J)$ یک R ــ مدول‌چپ یکانی است که عمل R بـا $(rf)(x) = f(xr)$ تعریف می‌شود $(r,x \in R; f \in \mathrm{Hom}_{\mathbf{Z}}(R,J))$.

لم ۱۱۰۳ . هرگاه J یک گروه آبلی بخشپذیر بوده و R حلقه‌ای یکدار باشد ، آنگاه $Hom_{\mathbf{Z}}(R,J)$ یک R ــ مدول چپ انژکتیو است .

طرح برهان . بنابر لم ۸۰۳ ، کافی است نشان دهیم که به‌ازای هر ایده‌آل چپ L از R ، هر همریختی $f : L \to \mathrm{Hom}_{\mathbf{Z}}(R,J)$ از R ــ مدولها را می‌توان به یک همریختی $h : R \to \mathrm{Hom}_{\mathbf{Z}}(R,J)$ از R ــ مدولها توسیع داد . نگاشت $g : L \to J$ داده شده با $g(a) = [f(a)](1_R)$ یک همریختی گروههاست . چون بنابر لم ۹۰۳ J یک $\mathbf{Z}$ ــ مدول انژکتیو است،باتوجه به نمودار

$$\begin{array}{ccc} 0 \to L & \xrightarrow{\subseteq} & R \\ & {\scriptstyle g}\downarrow & \\ & J & \end{array}$$

یک همریختی گروهها مانند $\bar{g} : R \to J$ وجود دارد به‌طوری که $\bar{g} \mid L = g$. $h : R \to \mathrm{Hom}_{\mathbf{Z}}(R,J)$ را با $r \mapsto h(r)$ تعریف می‌کنیم ، که در آن $h(r) : R \to J$ نگاشتی است که با $(x \in R)\ [h(r)](x) = \bar{g}(xr)$ داده می‌شود . تحقیق کنید که h تابع تعریف شده‌ای است (یعنی ، هر $h(r)$ یک همریختی گروهها مانند $R \to J$ است) و h یک همریختی گروهها مانند $R \to \mathrm{Hom}_{\mathbf{Z}}(R,J)$ می‌باشد . هرگاه $s,r,x \in R$ ، آنگاه

$$h(sr)(x) = \bar{g}(x(sr)) = \bar{g}((xs)r) = h(r)(xs).$$

طبق تعریف ساختار R ــ مدولی $\mathrm{Hom}_{\mathbf{Z}}(R,J)$ ، داریم $h(r)(xs) = [sh(r)](x)$ ، که از آنجا $h(sr) = sh(r)$ و h یک همریختی R ــ مدولهاست . بالاخره ، فرض کنیم $r \in L$ و $x \in R$. در این صورت ، $xr \in L$ و

$$h(r)(x) = \bar{g}(xr) = g(xr) = [f(xr)](1_R).$$

چون f یک همریختی R ــ مدولهاست و $\mathrm{Hom}_{\mathbf{Z}}(R,J)$ یک R ــ مدول است ،

$$[f(xr)](1_R) = [xf(r)](1_R) = f(r)(1_R x) = f(r)(x).$$

بنابراین ، به‌ازای $r \in L$ ، $h(r) = f(r)$ و h یک توسیع f می‌باشد .

حال قادریم دوگانهای نتیجهٔ ۳۰۳ و قضیهٔ ۴۰۳ را ثابت کنیم .

حکم ۱۲۰۳ . هر مدول یگانی A روی حلقهٔ یکدار R را می‌توان در یک R ــ مدول انژکتیو نشانید .

طرح برهان . چون A آبلی است ، بنابر لم ۱۰۰۳ ، یک گروه بخشپذیر مانند J و یک تکریختی گروهها چون $f : A \to J$ وجود دارند . به‌آسانی معلوم می‌شود که نگاشت $\bar{f} : \mathrm{Hom}_{\mathbf{Z}}(R,A) \to \mathrm{Hom}_{\mathbf{Z}}(R,J)$ داده شده با $\bar{f}(g) = fg \in \mathrm{Hom}_{\mathbf{Z}}(R,J)$ به‌ازای هر $g \in \mathrm{Hom}_{\mathbf{Z}}(R,A)$ یک همریختی R ــ مدولهاست . چون هر همریختی R ــ مدولها یک همریختی $\mathbf{Z}$ ــ مدولهاست ، داریم $\mathrm{Hom}_R(R,A) \subset \mathrm{Hom}_{\mathbf{Z}}(R,A)$. درواقع ، به‌آسانی معلوم می‌شود که $\mathrm{Hom}_R(R,A)$ یک R ــ زیرمدول $\mathrm{Hom}_{\mathbf{Z}}(R,A)$ است . بالاخره ، تحقیق کنید که نگاشت $A \to \mathrm{Hom}_R(R,A)$ داده شده با $a \mapsto f_a$ ، که $f_a(r) = ra$ ، یک تکریختی R ــ مدولهاست ، (درواقع ، یکریختی است) . ترکیب این نگاشتها تکریختی

$$A \to \mathrm{Hom}_R(R,A) \xrightarrow{\subseteq} \mathrm{Hom}_{\mathbf{Z}}(R,A) \xrightarrow{\bar{f}} \mathrm{Hom}_{\mathbf{Z}}(R,J)$$

از R ــ مدولها را به دست می‌دهد . چون $\mathrm{Hom}_{\mathbf{Z}}(R,J)$ ، طبق‌لم ۱۱۰۳ ، یک R ــ مدول انژکتیو است ، A در یک انژکتیو نشانیده شده است .

حکم ۱۳۰۳ . فرض کنیم R یک حلقهٔ یکدار باشد . شرایط زیر بر R ــ مدول یگانی J معادلند :

(یک) J انژکتیو است ؛

(دو) هر دنبالهٔ کامل کوتاه $0 \to J \xrightarrow{f} B \xrightarrow{g} C \to 0$ کامل تجزیه است . (از اینرو ، $B \cong J \oplus C$) ؛

(سه) J جمعوند مستقیم هر مدول B است که زیرمدولی از آن باشد .

طرح برهان . (دو) $\Rightarrow$ (یک) برهان (دو) $\Rightarrow$ (یک) قضیهٔ ۴۰۳ را دوگان می‌سازیم . (سه) $\Rightarrow$ (دو) چون دنبالهٔ $0 \to J \xrightarrow{\subseteq} B \xrightarrow{\pi} B/J \to 0$ کامل تجزیه است ، یک همریختی مانند $g : B/J \to B$ وجود دارد به‌طوری که $\pi g = 1_{B/J}$. بنابر قضیهٔ ۱۸۰۱ ((سه) $\Rightarrow$ (یک)) ، یکریختی مانند $J \oplus B/J \cong B$ وجوددارد که با $(x,y) \mapsto x + g(y)$

داده می‌شود. به آسانی معلوم می‌شود که B مجموع مستقیم داخلی J و $g(B/J)$ است. (یک) $\Rightarrow$ (سه) از حکم ۱۲.۳ نتیجه می‌شود که J زیرمدول یک مدول انژکتیو مانند Q است. حکم ۷.۳ و قسمت (سه) ایجاب می‌کنند که J انژکتیو باشد.

تمرینات

تذکر. R یک حلقه است. اگر R یکدار باشد، تمام R ــ مدولها یکانی فرض می‌شوند.

۱. شرایط زیر بر حلقهٔ R [دارای واحد] معادلند:
(آ) هر R ــ مدول [یکانی] تصویری است؛
(ب) هر دنبالهٔ کامل کوتاه از R ــ مدولها [ی یکانی] کامل تجزیه است.
(پ) هر R ــ مدول [یکانی] انژکتیو است.

۲. فرض کنید R حلقه‌ای یکدار باشد. R ــ مدول A انژکتیو است اگر و فقط اگر به‌ازای هر ایده‌آل چپ L از R و همریختی $g: L \to A$ از R ــ مدولها، $a \in A$ ای موجود باشد به‌طوری‌که به‌ازای هر $r \in L$ ، $g(r) = ra$.

۳. هر فضای برداری روی یک حلقهٔ بخشی D یک D ــ مدول تصویری وانژکتیو است. [ر.ک. تمرین ۱۰]

۴. (آ) به‌ازای هر p اول، $Z(p^\infty)$ (ر.ک. تمرین I.۱۰.۱۰) یک گروه بخشپذیر است.
(ب) هیچ گروه آبلی متناهی ناصفر بخشپذیر نیست.
(پ) هیچ گروه آبلی آزاد ناصفر بخشپذیر نیست.
(ت) $\mathbf{Q}$ یک گروه آبلی بخشپذیر است.

۵. $\mathbf{Q}$ یک $\mathbf{Z}$ ــ مدول تصویری نیست.

۶. هرگاه G گروهی آبلی باشد، آنگاه $G = D \oplus N$ ، که در آن D بخشپذیر بوده و N تحویل یافته است (بدین معنی که N زیرگروه بخشپذیر نابدیهی ندارد).
[**راهنمایی.** فرض کنید D زیرگروه تولید شده به وسیلهٔ اجتماع تمام زیرگروههای بخشپذیر G باشد.]

۷. بدون استفاده از لم ۹.۳، ثابت کنید که
(آ) هر نقش همریخت یک گروه آبلی بخشپذیر بخشپذیر است.
(ب) هر جمعوند مستقیم (تمرین I.۱۲.۸۰) یک گروه آبلی بخشپذیر

است.

(پ) هر مجموع مستقیم گروههای آبلی بخشپذیر بخشپذیر است.

۸. هر گروه آبلی بخشپذیر فارغ از تاب D مجموع مستقیمی است از نسخه‌های اعداد گویای $\mathbf{Q}$. [**راهنمایی.** هرگاه $0 \neq n \in \mathbf{Z}$ و $a \in D$، آنگاه یک $b \in D$ منحصر به فرد وجود دارد به‌طوری‌که $nb = a$. b را با $(1/n)a$ نشان دهید. به‌ازای $m, n \in \mathbf{Z}$ $(n \neq 0)$، تعریف کنید $(m/n)a = m(1/n)a$. در این صورت، D یک فضای برداری روی $\mathbf{Q}$ است. از قضیهٔ ۴۰۲ استفاده کنید.]

۹. (آ) هرگاه D گروهی آبلی و D_t زیرگروه‌تابی آن باشد، آنگاه D/D_t فارغ از تاب است.

(ب) هرگاه D بخشپذیرباشد، آنگاه D_t نیزچنین‌است، که‌ازآنجا $D = D_t \oplus E$، که در آن E فارغ از تاب می‌باشد.

۱۰. فرض کنید p اول بوده و D یک p ـ‌گروه آبلی بخشپذیر باشد. در این صورت، D یک مجموع مستقیم نسخه‌های $Z(p^\infty)$ است. [**راهنمایی.** فرض کنید X پایه‌ای از فضای برداری $D[p]$ روی Z_p باشد (ر.ک. تمرین ۴۰۲). هرگاه $x \in X$، آنگاه $x_1, x_2, x_3, \ldots \in D$ وجود دارند به‌طوری که

$$x_1 = x, |x_1| = p, \quad px_2 = x_1, \quad px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots.$$

هرگاه H_x زیرگروه تولید شده به وسیلهٔ x_i باشد، آنگاه، بنابر تمرین ۷۰۳۰ I، $H_x \cong Z(p^\infty)$. نشان دهید که $D \cong \sum_{x \in X} H_x$.]

۱۱. هر گروه آبلی بخشپذیر یک مجموع مستقیم نسخه‌هایی از اعداد گویای $\mathbf{Q}$ و نسخه‌هایی از $Z(p^\infty)$ به‌ازای مقادیر مختلف p است. [**راهنمایی.** تمرین ۹ را در مورد D و تمرینهای ۷ و ۸ را در مورد جمعوند فارغ از تاب به دست آمده به کار گیرید. بنابر تمرینهای ۷، ۱۰، و ۷۰۲۰ II، جمعوند دیگر D_t مجموع مستقیمی از نسخه‌های مختلف $Z(p^\infty)$ است.]

۱۲. فرض کنید G, H, K گروههای آبلی بخشپذیری باشند.

(آ) هرگاه $G \oplus G \cong H \oplus H$، آنگاه $G \cong H$ [ر.ک. تمرین ۱۱].

(ب) هرگاه $G \oplus H \cong G \oplus K$، آنگاه $H \cong K$ [ر.ک. تمرینات ۱۱ و ۱۱۰۲۰ II].

۱۳ . اگر بخواهیم مفهوم مدول آزاد روی حلقهٔ R را دوگان سازیم (و شیٔ تعریف شده به‌این‌صورت‌را "هم‌آزاد" بنامیم)، تعریف خواهد بود: R ــ مدول F بر مجموعهٔ X هم‌آزاد است اگرتابعی مانند $\iota : X \to F$، وجود داشته باشد به‌طوری‌که به‌ازای هر R ــ مدول A و تابع $f : A \to X$، یک همریختی منحصر به فرد از مدولها مانند $\bar{f} : A \to F$ موجود باشد به‌طوری که $\bar{f}\iota = f$ (ر.ک. قضیهٔ ۱۰۲ (چهار)). نشان دهید که به‌ازای هر مجموعهٔ X که $|X| \geq 2$، یک‌چنین R ــ مدول F وجودندارد. هرگاه $|X| = 1$، آنگاه 0 تنهامدول‌هم‌آزاد است. [**راهنمایی.** اگر F موجود بوده و $|X| \geq 2$، باتوجه‌به‌نقشهای ممکن 0 و ساختن $f : R \to X$ به‌طوری‌که به‌ازای هر همریختی $\bar{f} : R \to F$، $\bar{f}\iota \neq f$، به تناقض برسید.]

۱۴ . هرگاه D حلقه‌ای یکدار باشد به‌طوری‌که هر D ــ مدول یکانی آزاد باشد، آنگاه D یک حلقهٔ بخشی است. [**راهنمایی.** بنابر تمرین III ۷.۲۰ و قضیهٔ III ۱۸.۲۰، کافی است نشان دهید که D ایده‌آل چپ ماکزیمال ناصفر ندارد. توجه کنید که بنابرقضیهٔ ۲.۳، تمرین ۱، و حکم ۱۳.۳، هر ایده‌آل چپ D یک D ــ مدول آزاد، و درنتیجه یک جمعوند مستقیم (مدولی) $\dot{D}$ است.]

۴ HOM و دوگانی

ابتدا رفتار $\mathrm{Hom}_R(A,B)$ را نسبت به نگاشتهای القایی، دنباله‌های کامل، مجموعهای مستقیم، و حاصل‌ضربهای مستقیم مورد بحث قرار می‌دهیم. آخرین قسمت از بخش، که اساسا" از قسمت اول مستقل است، با دوگانی سر و کار دارد.

به یاد آورید که هرگاه A و B مدولهایی روی حلقهٔ R باشند، آنگاه $\mathrm{Hom}_R(A,B)$ مجموعهٔ تمام همریختیهای R ــ مدولهای $f : A \to B$ است. اگر $R = \mathbf{Z}$، معمولا" به جای $\mathrm{Hom}_{\mathbf{Z}}(A,B)$ می‌نویسیم $\mathrm{Hom}(A,B)$. $\mathrm{Hom}_R(A,B)$ یک گروه‌آبلی تحت جمع است و این جمع نسبت به ترکیب توابع پخشپذیر می‌باشد (ر.ک. ص ۲۷۲).

قضیهٔ ۱۰۴ . *فرض کنیم* A,B,C,D *مدولهایی روی حلقهٔ* R *بوده و* $\varphi : C \to A$ *و* $\psi : B \to D$ *همریختیهایی از* R ــ *مدولها باشند. در این صورت، نگاشت* $\theta : Hom_R(A,B) \to Hom_R(C,D)$ *داده شده با* $f \mapsto \psi f \varphi$ *یک همریختی گروههای آبلی خواهد بود.*

طرح برهان. θ تعریف شده است، زیرا ترکیب همریختیهای R ــ مدولها یک همریختی R ــ مدولهاست. θ یک همریختی است، زیرا این ترکیب همریختیها نسبت به جمع پخشپذیر است.

نگاشت θ در قضیهٔ ۱۰۴ معمولاً با $\mathrm{Hom}(\varphi,\psi)$ نموده و همریختی القا شده به وسیلهٔ φ و ψ نامیده می‌شود. توجه کنید که به‌ازای همریختیهای $\varphi_1 : E \to C, \varphi_2 : C \to A, \psi_1 : B \to D, \psi_2 : D \to F$،

$$\mathrm{Hom}(\varphi_1,\psi_2)\,\mathrm{Hom}(\varphi_2,\psi_1) = \mathrm{Hom}(\varphi_2\varphi_1,\psi_2\psi_1) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(E,F).$$

دو حالت خاص مهم از همریختی القایی وجود دارد. هرگاه $B = D$ و $\psi = 1_B$، آنگاه نگاشت القایی $\mathrm{Hom}(\varphi,1_B) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(C,B)$ با $f \mapsto f\varphi$ داده شده و با $\bar{\varphi}$ نموده می‌شود. به همین نحو، اگر $A = C$ و $\varphi = 1_A$، نگاشت القایی $\mathrm{Hom}(1_A,\psi) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(A,D)$ با $f \mapsto \psi f$ داده شده و با $\bar{\psi}$ نموده می‌شود.

حال رفتار Hom_R را در مورد دنباله‌های کامل بررسی می‌کنیم.

قضیهٔ ۲۰۴. *فرض کنیم R یک حلقه باشد. $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ یک دنبالهٔ کامل از R ــ مدولهاست اگر و فقط اگر به‌ازای هر R ــ مدول D،*

$$0 \to Hom_R(D,A) \xrightarrow{\bar{\varphi}} Hom_R(D,B) \xrightarrow{\bar{\psi}} Hom_R(D,C)$$

یک دنبالهٔ کامل از گروههای آبلی باشد.

برهان. اگر $A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ کامل باشد، باید ثابت کنیم: (یک) $\mathrm{Ker}\,\bar{\varphi} = 0$ (یعنی، $\bar{\varphi}$ یک تکریختی است)؛ (دو) $\mathrm{Im}\,\bar{\varphi} \subset \mathrm{Ker}\,\bar{\psi}$؛ و (سه) $\mathrm{Ker}\,\bar{\psi} \subset \mathrm{Im}\,\bar{\varphi}$.

(یک) به‌ازای هر $x \in D$، $f \in \mathrm{Ker}\,\bar{\varphi} \Rightarrow \varphi f = 0 \Rightarrow \varphi f(x) = 0$. چون $0 \to A \xrightarrow{\varphi} B$ کامل است، φ تکریختی است؛ درنتیجه به‌ازای هر $x \in D$، $f(x) = 0$ و لذا $f = 0$. بنابراین، $\mathrm{Ker}\,\bar{\varphi} = 0$.

(دو) چون بنابر کامل بودن $\mathrm{Im}\,\varphi = \mathrm{Ker}\,\psi$، داریم $\psi\varphi = 0$؛ و درنتیجه، $\bar{\psi}\bar{\varphi} = \overline{\psi\varphi} = 0$. بنابراین، $\mathrm{Im}\,\bar{\varphi} \subset \mathrm{Ker}\,\bar{\psi}$.

(سه) $g \in \mathrm{Ker}\,\bar{\psi} \Rightarrow \psi g = 0 \Rightarrow \mathrm{Im}\,g \subset \mathrm{Ker}\,\psi = \mathrm{Im}\,\varphi$. چون φ تکریختی است، $\varphi : A \to \mathrm{Im}\,\varphi$ یکریختی می‌باشد. هرگاه h ترکیب $D \xrightarrow{g} \mathrm{Im}\,g \subset \mathrm{Im}\,\varphi \xrightarrow{\varphi^{-1}} A$ باشد، آنگاه $h \in \mathrm{Hom}_R(D,A)$ و $g = \varphi h = \bar{\varphi}(h)$. بنابراین، $\mathrm{Ker}\,\bar{\psi} \subset \mathrm{Im}\,\bar{\varphi}$.

به‌عکس، فرض کنیم دنباله‌ٔ ساخته شده با جملات Hom و نگاشتهای القایی به‌ازای هر D کامل‌باشد. ابتدا فرض کنیم که $D = \operatorname{Ker}\varphi$ و $i : D \to A$ نگاشت شمول باشد. چون $\operatorname{Ker}\bar{\varphi} = 0$ (کامل‌بودن) و $\bar{\varphi}(i) = \varphi i = 0$، بایدداشته باشیم $i = 0$، که ایجاب می‌کند که $D = \operatorname{Ker}\varphi = 0$. بنابراین، $0 \to A \xrightarrow{\varphi} B$ کامل‌است. حال فرض کنیم $D = A$. چون $\operatorname{Ker}\bar{\psi} = \operatorname{Im}\bar{\varphi}$، داریـــم $0 = \bar{\psi}\bar{\varphi}(1_A) = \psi\varphi 1_A = \psi\varphi$، کـه از آنجا $\operatorname{Im}\varphi \subset \operatorname{Ker}\psi$. بالاخره، فرض کنیم $D = \operatorname{Ker}\psi$ و $j : D \to B$ نگاشت‌شمول باشد. چون $0 = \psi j = \bar{\psi}(j)$ و $\operatorname{Ker}\bar{\psi} = \operatorname{Im}\bar{\varphi}$، به‌ازای $f : D \to A$ ی داریم $j = \bar{\varphi}(f) = \varphi f$. بنابراین، به‌ازای هر $x \in D = \operatorname{Ker}\psi$، $x = j(x) = \varphi f(x) \in \operatorname{Im}\varphi$ و $\operatorname{Ker}\psi \subset \operatorname{Im}\varphi$. لذا، $\operatorname{Ker}\psi = \operatorname{Im}\varphi$ و $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ کامل است.

حکم ۳۰۴. *فـرض کنیـم* R *یک حلقـه بـاشـد.* $A \xrightarrow{\theta} B \xrightarrow{\zeta} C \to 0$ *یک دنبالهٔ کامل از* R *ــ مدولهاست اگر و فقط اگر به‌ازای هر* R *ــ مدول* D،

$$0 \to Hom_R(C,D) \xrightarrow{\bar{\zeta}} Hom_R(B,D) \xrightarrow{\bar{\theta}} Hom_R(A,D)$$

یک دنبالهٔ کامل از گروههای آبلی باشد.

طرح برهان. اگر $A \xrightarrow{\theta} B \xrightarrow{\zeta} C \to 0$ کامل بـاشد، نشـان می‌دهیم که $\operatorname{Ker}\bar{\theta} \subset \operatorname{Im}\bar{\zeta}$. هرگاه $f \in \operatorname{Ker}\bar{\theta}$، آنگاه $0 = \bar{\theta}(f) = f\theta$، کـه از آنجا $f(\operatorname{Im}\theta) = f(\operatorname{Ker}\zeta) = 0$. بنابر قضیهٔ ۷۰۱، f همریختی $\bar{f} : B/\operatorname{Ker}\zeta \to D$ رااالقامی‌کندبه‌طوری‌که $\bar{f}(b + \operatorname{Ker}\zeta) = f(b)$. مجددا" بنابر قضیهٔ ۷۰۱، یک یکریختی مانند $\varphi : B/\operatorname{Ker}\zeta \cong C$ وجود دارد به‌طوری که $\varphi(b + \operatorname{Ker}\zeta) = \zeta(b)$. بنابراین، نگاشت $\bar{f}\varphi^{-1} : C \to D$ یک همریختی R ــ مدولهاست به‌طوری‌که $\bar{\zeta}(\bar{f}\varphi^{-1}) = f$. از اینرو، $\operatorname{Ker}\bar{\theta} \subset \operatorname{Im}\bar{\zeta}$. باقیماندهٔ این نیمهٔ برهان مشـابه برهان قضیهٔ ۲۰۴ است.

به عـکس، اگـر دنباله با جملات Hom به‌ازای هر D کامل باشد، فرض می‌کنیم $D = C/\operatorname{Im}\zeta$ و $\pi : C \to D$ تصویر کانـونی بـاشد. در ایـن صورت، $\bar{\zeta}(\pi) = \pi\zeta = 0$ و $\operatorname{Ker}\bar{\zeta} = 0$ ایجاب می‌کنندکه $\pi = 0$، که ازآنجا $C = \operatorname{Im}\zeta$ و درنتیجه $B \xrightarrow{\zeta} C \to 0$ کامل است. به همین نحـو، با قرار دادن $D = B/\operatorname{Im}\theta$ و با در نظر گرفتن برووریختی کانونی $B \to D$، نشان‌دهیدکه $\operatorname{Ker}\zeta \subset \operatorname{Im}\theta$. بالاخره، هرگاه $D = C$، آنگاه $0 = \bar{\theta}\bar{\zeta}(1_C) = \zeta\theta$، که از آنجا $\operatorname{Im}\theta \subset \operatorname{Ker}\zeta$. بنابراین، $A \xrightarrow{\theta} B \xrightarrow{\zeta} C \to 0$ کامل می‌باشد.

گاهی دو نتیجهٔ فوق را خلاصه کرده و می‌گوییم $\mathrm{Hom}_R(A,B)$ *کامل چپ* است. در حالت کلی دنبالهٔ کامل کوتاه $0 \to A \to B \to C \to 0$ دنبالهٔ کامل کوتاه $0 \to \mathrm{Hom}_R(D,A) \to \mathrm{Hom}_R(D,B) \to \mathrm{Hom}_R(D,C) \to 0$ را القا نمی‌کند (و به همین ترتیب در مورد متغیر اول؛ ر.ک. تمرین ۳). اما سه قضیهٔ زیر نشان‌می‌دهند که این نتیجه در چند حالت برقرار است.

حکم ۴.۴. *شرایط زیر بر مدولها روی حلقهٔ* R *معادلند:*

(یک) $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *یک دنبالهٔ کامل تجزیه از* R*ـ مدولهاست؛*

(دو) *به‌ازای هر* R*ـ مدول* D، $0 \to Hom_R(D,A) \xrightarrow{\bar{\varphi}} Hom_R(D,B) \xrightarrow{\bar{\psi}} Hom_R(D,C) \to 0$ *یک دنبالهٔ کامل تجزیه، از گروههای آبلی است؛*

(سه) *به‌ازای هر* R*ـ مدول* D، $0 \to Hom_R(C,D) \xrightarrow{\bar{\psi}} Hom_R(B,D) \xrightarrow{\bar{\varphi}} Hom_R(A,D) \to 0$ *یک دنبالهٔ کامل تجزیه از گروههای آبلی است.*

طرح برهان. (سه) $\Rightarrow$ (یک) بنابر قضیهٔ ۱.۱، یک همریختی مانند $\alpha : B \to A$ وجود دارد به‌طوری‌که $\alpha\varphi = 1_A$. تحقیق کنید که همریختی القایی

$$\bar{\alpha} : \mathrm{Hom}_R(A,D) \to \mathrm{Hom}_R(B,D)$$

چنان است که $\bar{\varphi}\bar{\alpha} = 1_{\mathrm{Hom}_R(A,D)}$. درنتیجه، $\bar{\varphi}$ یک‌بروریختی است (آشنایی، قضیهٔ ۱.۳) و، بنابر حکم ۳.۴ و قضیهٔ ۱.۱، دنبالهٔ ساخته شده با Hom_R یک دنبالهٔ کامل تجزیه است. (یک) $\Rightarrow$ (سه) هرگاه $D = A$ و $f : B \to A$ چنان باشد که $\bar{\varphi}(f) = f\varphi = 1_A$، آنگاه φ تکریختی است (آشنایی، قضیهٔ ۱.۳) و، بنابر حکم ۳.۴ و قضیهٔ ۱.۱، $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ دنبالهٔ کامل‌تجزیه است. نتایج دیگر به همین نحو ثابت می‌شوند.

قضیهٔ ۵.۴. *شرایط زیر بر مدول* P *روی حلقهٔ* R *باهم معادلند:*

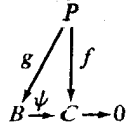
(یک) P *تصویری است؛*

(دو) *هرگاه* $\psi : B \to C$ *یک‌بروریختی* R*ـ مدولها باشد، آنگاه* $\bar{\psi} : Hom_R(P,B) \to Hom_R(P,C)$ *یک بروریختی گروههای آبلی است؛*

(سه) *هرگاه* $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *یک دنبالهٔ کامل کوتاه از* R*ـ مدولها باشد، آنگاه*

$0 \to Hom_R(P,A) \xrightarrow{\bar{\varphi}} Hom_R(P,B) \xrightarrow{\bar{\psi}} Hom_R(P,C) \to 0$ یک دنبالهٔ کامل از گروههای آبلی است.

طرح برهان. (دوم) $\Leftrightarrow$ (یک) نگاشت $\bar{\psi} : \mathrm{Hom}_R(P,B) \to \mathrm{Hom}_R(P,C)$ (داده شده با $g \mapsto \psi g$) بروریختی است اگر و فقط اگر به‌ازای هر همریختی R ــ مدولها مانند $f : P \to C$. یک همریختی R ــ مدولها مانند $g : P \to B$ موجود باشد به‌طوری‌که نمودار



تعویض‌پذیر باشد (یعنی، $f = \psi g = \bar{\psi}(g)$) . (سه) $\Rightarrow$ (دو) قضیهٔ ۲۰۴ . (دو) $\Rightarrow$ (سه) با معلوم بودن بروریختی $\psi : B \to C$ ، فرض کنید $A = \mathrm{Ker}\,\psi$ و قسمت (سه) را در مورد دنبالهٔ کامل کوتاه $0 \to A \xrightarrow{\subseteq} B \xrightarrow{\psi} C \to 0$ به کار برید.

حکم ۶۰۴ . شرایط زیر بر مدول J روی حلقهٔ R معادلند:

(یک) J انژکتیو است؛

(دو) هرگاه $\theta : A \to B$ یک تکریختی R ــ مدولها باشد، آنگاه $\bar{\theta} : Hom_R(B,J) \to Hom_R(A,J)$ یک بروریختی گروههای آبلی است؛

(سه) هرگاه $0 \to A \xrightarrow{\theta} B \xrightarrow{\xi} C \to 0$ یک دنبالهٔ کامل کوتاه از R ــ مدولها باشد، آنگاه $0 \to Hom_R(C,J) \xrightarrow{\bar{\xi}} Hom_R(B,J) \xrightarrow{\bar{\theta}} Hom_R(A,J) \to 0$ یک دنبالهٔ کامل از گروههای آبلی است.

برهان. اثبات دوگان برهان قضیهٔ ۵۰۴ است و به عنوان تمرین گذارده می‌شود.

قضیهٔ ۷۰۴ . فرض کنیم A ، B ، $\{A_i \mid i \in I\}$ ، و $\{B_j \mid j \in J\}$ مدولهایی روی حلقهٔ R باشند. در این صورت، یکریختیهای زیر از گروههای آبلی وجود دارند:

(یک) $Hom_R(\sum_{i \in I} A_i, B) \cong \prod_{i \in I} Hom_R(A_i, B)$ ؛

(دو) $Hom_R(A, \prod_{j \in J} B_j) \cong \prod_{j \in J} Hom_R(A, B_j)$ ؛

چند تبصره. هرگاه I و J متناهی باشند، آنگاه $\sum_{i\in I} A_i = \prod_{i\in I} A_i$ و $\sum_{j\in J} B_j = \prod_{j\in J} B_j$.
اما اگر I و J نامتناهی باشند، قضیه در صورت تعویض حاصلضرب مستقیم $\prod$ با مجموع مستقیم $\sum$ ممکن است درست نباشد (ر.ک. تمرین ۱۰).

طرح برهان ۷.۴. (یک) به‌ازای هر $i\in I$، فرض کنیم $\iota_i : A_i \to \sum_{i\in I} A_i$ انژکسیون کانونی باشد (قضیهٔ ۱۱.۱). به‌ازای $\{g_i\} \in \prod_{i\in I} \mathrm{Hom}_R(A_i,B)$، یک همریختی منحصر به فرد از R ــ مدولها مانند $g : \sum_{i\in I} A_i \to B$ وجود دارد به‌طوری که به‌ازای هر $i\in I$، $g\iota_i = g_i$ (قضیهٔ ۱۳.۱). تحقیق کنید که نگاشت $\psi : \prod \mathrm{Hom}_R(A_i,B) \to \mathrm{Hom}_R(\sum A_i,B)$ داده شده با $g \mapsto \{g_i\}$ یک همریختی است. نشان دهید که نگاشت $\varphi : \mathrm{Hom}_R(\sum A_i,B) \to \prod \mathrm{Hom}_R(A_i,B)$ داده‌شده با $f \mapsto \{f_i\}$ یک همریختی است به‌طوری که $\varphi\psi$ و $\psi\varphi$ نگاشتهایی همانی‌اند. لذا، φ یک یکریختی است. قسمت (دو) به همین نحو با قضیهٔ ۱۲.۱ به جای قضیهٔ ۱۳.۱ ثابت می‌شود.

برای پرداختن به دوگانی و مفاهیم دیگر، باید ساختارهای مدولی ممکن بر گروه آبلی $\mathrm{Hom}_R(A,B)$ را درنظر بگیریم. موضوع را با چند مطلب در باب دو مدولها آغاز می‌کنیم. فرض کنیم R و S حلقه باشند. گروه آبلی A یک **R-S دو مدول** است مشروط بر آنکه A هم R ــ مدول چپ و هم S ــ مدول راست بوده و

$$r(as) = (ra)s \quad ،\quad a\in A, r\in R, s\in S$$

به‌ازای هر .

گاهی برای نشان دادن اینکه A یک R-S دو مدول است می‌نویسیم ${}_RA_S$. به همین نحو، ${}_RB$ یعنی یک R ــ مدول چپ B و C_S یعنی یک S ــ مدول راست C.

چند مثال. هر حلقهٔ R دارای ضرب شرکتپذیر است؛ و درنتیجه، یک R-R دو مدول است، هر مدول چپ A روی حلقهٔ تعویضپذیر R یک R-R دو مدول است با $ra = ar$ $(a\in A, r\in R)$.

قضیهٔ ۸۰۴ . *فرض کنیم* R و S *حلقه‌هایی بوده و* ${}_RA_S, {}_RB_S, {}_RC_S, {}_RD$ *(دو) مدولهای مربوطه باشند .*

(یک) $Hom_R(A,B)$ *یک* S *ـ مدول راست است که در آن عمل* S *با* $(fs)(a) = (f(a))s$ $(s \in S; a \in A; f \in Hom_R(A,B))$ *داده شده است .*

(دو) *هرگاه* $\varphi : A \to A'$ *یک همریختی از* R *ـ مدولهای چپ باشد ، آنگاه نگاشت القایی* $\bar{\varphi} : \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B)$ *یک همریختی از* S *ـ مدولهای راست است .*

(سه) $Hom_R(C,D)$ *یک* S *ـ مدول چپ است که در آن عمل* S *با* $(sg)(c) = g(cs)$ $(s \in S; c \in C; g \in Hom_R(C,D))$ *داده شده است .*

(چهار) *هرگاه* $\psi : D \to D'$ *یک همریختی از* R *ـ مدولهای چپ باشد ، آنگاه* $\bar{\psi} : Hom_R(C,D) \to Hom_R(C,D')$ *یک همریختی از* S *ـ مدولهای چپ است .*

طرح برهان . (یک) تحقیق این امر که fs یک همریختی تعریف شده از مدولها بوده و $\mathrm{Hom}_R(A,B)$ درواقع یک S ـ مدول راست است خسته کننده ولی سرراست است ؛ به همین نحو ، در مورد (سه) . (دو) بنابر قضیهٔ ۸۰۴ . ۱ ، $\bar{\varphi}$ یک همریختی گروههای آبلی است . هرگاه $f \in \mathrm{Hom}_R(A',B)$ ، $a \in A$ و $s \in S$ ، آنگاه

$$\bar{\varphi}(fs)(a) = ((fs)\varphi)(a) = (fs)(\varphi(a)) = (f(\varphi(a)))s = (f\varphi(a))s = ((\bar{\varphi}f)(a))s.$$

از اینرو ، $\bar{\varphi}(fs) = (\bar{\varphi}f)s$ و $\bar{\varphi}$ یک‌همریختی از S ـ مدولهای راست است . قسمت (چهار) به نحو مشابه ثابت می‌شود .

تبصره . یک حالت خاص مهم از قضیهٔ ۸۰۴ وقتی رخ می‌دهد که R تعویضپذیر است ؛ و درنتیجه ، هر R ـ مدول C یک R-R دو مدول با $rc = cr$ $(r \in R, c \in C)$ می‌باشد . در این حالت ، به‌ازای هر $r \in R$ ، $a \in A$ ، و $f \in \mathrm{Hom}_R(A,B)$ ، داریم

$$(rf)(a) = f(ar) = f(ra) = rf(a) = (f(a))r = (fr)(a).$$

پس نتیجه می‌شود که $\mathrm{Hom}_R(A,B)$ یک R-R دو مدول است ، که در آن به‌ازای هر $r \in R, f \in \mathrm{Hom}_R(A,B)$ ، $rf = fr$.

قضیهٔ ۹۰۴ . *هرگاه* A *یک مدول چپ یکانی روی حلقهٔ یکدار* R *باشد ، آنگاه یک یکریختی از* R *ـ مدولهای چپ مانند* $A \cong Hom_R(R,A)$ *وجود دارد .*

طرح برهان. چون R یک R-R دومدول‌است، ساختار مدولی چپ $\mathrm{Hom}_R(R,A)$ به‌وسیلهٔ قضیهٔ ۸.۴ (سه) داده می‌شود. تحقیق کنید که نگاشت $\varphi : \mathrm{Hom}_R(R,A) \to A$ داده شده با $f \mapsto f(1_R)$ یک‌همریختی‌از R ــ مدولهاست. نگاشت $\psi : A \to \mathrm{Hom}_R(R,A)$ را با $a \mapsto f_a$ تعریف می‌کنیم، کــه در آن $f_a(r) = ra$. تحقیق کنید که ψ یک همریختی تعریف شده از R ــ مدولها است به‌طوری‌که $\varphi\psi = 1_A$ و $\psi\varphi = 1_{\mathrm{Hom}_R(R,A)}$.

فرض کنیم A یک‌مدول‌چپ‌روی حلقهٔ R باشد. چون R یک R-R دو مدول است، بنابر قضیهٔ ۸.۴ (یک)، $\mathrm{Hom}_R(A,R)$ یک R ــ مدول راست می‌باشد. $\mathrm{Hom}_R(A,R)$ مدول **دوگان** A است و با A^* نموده می‌شود. عناصر A^* را گاهی **تابعیهای خطی** می‌نامند. به‌همین‌نحو، هرگاه B یک R ــ مدول راست باشد، آنگاه دوگان B^* از B، R ــ مدول **چپ** $\mathrm{Hom}_R(B,R)$ می‌باشد (تمرین ۴ (آ)).

قضیهٔ ۱۰.۴. *فرض کنیم A، B، و C مدولهای چپ روی حلقهٔ R باشند.*
(یک) هرگاه $\varphi : A \to C$ یک همریختی از R ــ مدولهای چپ باشد، آنگاه نگاشت القایی $\bar{\varphi} : C^* = Hom_R(C,R) \to Hom_R(A,R) = A^*$ یک همریختی از R ــ مدولهای‌راست است.
(دو) یک یکریختی از R ــ مدولها مانند $(A \oplus C)^* \cong A^* \oplus C^*$ وجود دارد.
(سه) هرگاه R حلقهٔ بخشی بوده و $0 \to A \xrightarrow{\theta} B \xrightarrow{\xi} C \to 0$ یک دنبالهٔ کامل کوتاه از فضاهای برداری چپ باشد، آنگاه $0 \to C^* \xrightarrow{\bar{\xi}} B^* \xrightarrow{\bar{\theta}} A^* \to 0$ یک دنبالهٔ کامل کوتاه از فضاهای برداری راست است.

برهان. تمرین؛ ر.ک. قضایای ۴.۲، ۲.۳، ۱.۴، ۵.۴، و ۷.۴. نگاشت $\bar{\varphi}$ در (یک) نگاشت دوگان φ نام دارد.

هرگاه A یک مدول چپ روی حلقهٔ R بوده، $a \in A$، و $f \in A^* = \mathrm{Hom}_R(A,R)$، آنگاه اعلب $f(a) \in R$ با $\langle a,f \rangle$ نموده می‌شود. چون f یک‌همریختی از R ــ مدولهاست،

$$\langle r_1a_1 + r_2a_2, f \rangle = r_1\langle a_1,f \rangle + r_2\langle a_2,f \rangle \qquad (r_i \in R,\ f \in A^*,\ a_i \in A). \tag{۱}$$

به همین نحو، چون A^* یک R ــ مدول راست با خاصیت $(fr)(a) = f(a)r$ است، داریم

(۲) $\langle a, f_1 r_1 + f_2 r_2 \rangle = \langle a, f_1 \rangle r_1 + \langle a, f_2 \rangle r_2 \qquad (r_i \in R, f_i \in A^*, a \in A).$

در برهانهای زیر از نماد کروشه برای تابعیهای خطی و نیز از **نماد دلتای کرونکر** استفاده می‌کنیم: به‌ازای هر مجموعهٔ اندیسگذار I و حلقهٔ یکدار R، علامت δ_{ij} $(i,j \in I)$ مبین $0 \in R$ است اگر $i \neq j$ و مساوی $1_R \in R$ است اگر $i = j$.

قضیهٔ ۱۱.۴. *فرض کنیم F یک مدول چپ آزاد روی حلقهٔ یکدار R باشد. همچنین، X پایه‌ای از F بوده و، به‌ازای هر $x \in X$، $f_x : F \to R$ با $(y \in X)\ f_x(y) = \delta_{xy}$ داده شده باشد. در این صورت،*

(یک) $\{f_x \mid x \in X\}$ یک زیرمجموعهٔ مستقل خطی F^* با اصلیت $|X|$ است؛

(دو) هرگاه X متناهی باشد، آنگاه F^* یک R ــ مدول راست آزاد با پایهٔ $\{f_x \mid x \in X\}$ است.

چند تبصره. همریختیهای f_x تعریف شده‌اند، زیرا F آزاد و با پایهٔ X است (قضیهٔ ۱۰۲). در قسمت (دو)، $\{f_x \mid x \in X\}$ **پایهٔ** دوگان X نام دارد. بنابر قضیهٔ ۴۰۲، این قضیه بوضوح برای هر فضای برداری V روی حلقهٔ بخشی درست است. بخصوص، هرگاه V با بعد متناهی باشد، آنگاه حکم ۹۰۲ و قضیهٔ ۱۱۰۴ ایجاب می‌کنند که $\dim V = \dim V^*$ و $V \cong V^*$. اما، هرگاه V با بعد نامتناهی باشد، آنگاه $\dim V^* > \dim V$ (تمرین ۱۲). به‌طورکلی، اگر F یک‌مدول آزاد روی یک حلقهٔ دلخواه (مثلاً "، $\mathbb{Z}$) باشد، F^* لزوماً آزاد نیست (ر.ک. تمرین ۱۰).

برهان ۱۱.۴. (یک) هرگاه $(r_i \in R;\ x_i \in X)\ f_{x_1} r_1 + f_{x_2} r_2 + \cdots + f_{x_n} r_n = 0$، آنگاه به‌ازای هر $j = 0,1,2,\ldots,n$،

$$0 = \langle x_j, 0 \rangle = \left\langle x_j, \sum_{i=1}^{n} f_{x_i} r_i \right\rangle = \sum_i \langle x_j, f_{x_i} \rangle r_i = \sum_i \delta_{ij} r_i = r_j.$$

چون به‌ازای هر j، $r_j = 0$، $\{f_x \mid x \in X\}$ مستقل خطی است. هرگاه $x \neq y \in X$، آنگاه $f_x(x) = 1_R \neq 0 = f_y(x)$، که از آنجا $f_x \neq f_y$. بنابراین، $|\{f_x \mid x \in X\}| = |X|$.

(دو) اگر X متناهی باشد، مثلاً $X = \{x_1, \ldots, x_n\}$، و $f \in F^*$، قرار می‌دهیم $s_i = f(x_i) = \langle x_i, f \rangle \in R$ و f_{x_i} را با f_i نشان می‌دهیم. هرگاه $u \in F$، آنگاه، به‌ازای

$$\text{و } u = r_1x_1 + r_2x_2 + \cdots + r_nx_n \in F \text{ ، ی } r_i \in R$$

$$\begin{aligned}\left\langle u, \sum_{j=1}^{n} f_j s_j \right\rangle &= \left\langle \sum_{i=1}^{n} r_i x_i, \sum_j f_j s_j \right\rangle \\ &= \sum_i \sum_j r_i \langle x_i, f_j \rangle s_j = \sum_i \sum_j r_i \delta_{ij} s_j = \sum_i r_i s_i \\ &= \sum_i r_i \langle x_i, f \rangle = \langle \sum_i r_i x_i, f \rangle = \langle u, f \rangle.\end{aligned}$$

بنابراین ، $f = f_1s_1 + f_2s_2 + \cdots + f_ns_n$ و $\{f_i\} = \{f_x \mid x \in X\}$ ، F^* را تولید می‌کند . از اینرو ، $\{f_x \mid x \in X\}$ یک پایه و F^* آزاد خواهد بود .

فرایند تشکیل دوگانها را می‌توان تکرار کرد . هرگاه A یک R ــ مدول چپ باشد ، آنگاه A^* یک R ــ مدول راست است و $A^{**} = (A^*)^* = \mathrm{Hom}_R(\mathrm{Hom}_R(A,R),R)$ (که در آن Hom_R سمت‌چپ‌مبین تمام همریختیهای R ــ مدولهای **راست** است) یک R ــ مدول چپ می‌باشد (ر.ک. تمرین ۴ (آ)) . A^{**} **دوگان مضاعف** A نامیده می‌شود .

قضیهٔ ۱۲.۴ . فرض کنیم A یک مدول چپ روی حلقهٔ R باشد .
(یک) یک همریختی از R ــ مدولها مانند $\theta : A \to A^{**}$ وجود دارد .
(دو) هرگاه R یکدار بوده و A آزاد باشد ، آنگاه θ یک تکریختی است .
(سه) هرگاه R یکدار بوده و A آزاد و دارای پایهٔ متناهی باشد ، آنگاه θ یک یکریختی است .

مدول A که در آن $\theta : A \to A^{**}$ یکریختی است منعکس نامیده می‌شود .

برهان ۱۲.۴ . (یک) به‌ازای هر $a \in A$ ، فرض کنیم $\theta(a) : A^* \to R$ نگاشت تعریف شده با $[\theta(a)](f) = \langle a,f \rangle \in R$ باشد . رابطهٔ (۲) پس از قضیهٔ ۱۰.۴ نشان می‌دهد که $\theta(a)$ یک همریختی از R ــ مدولهای راست است (یعنی ، $\theta(a) \in A^{**}$) . طبق رابطهٔ (۱) بعد از قضیهٔ ۱۰.۴ ، نگاشت $\theta : A \to A^{**}$ داده شده با $a \mapsto \theta(a)$ یک همریختی از R ــ مدولهاست .

(دو) فرض‌کنیم X پایه‌ای‌از A باشد . هرگاه $a \in A$ ، آنگاه $a = r_1x_1 + r_2x_2 + \cdots + r_nx_n$ $(r_i \in R; x_i \in X)$. هرگاه $\theta(a) = 0$ ، آنگاه ، به‌ازای هر $f \in A^*$ ،

$$0 = \langle a,f \rangle = \left\langle \sum_{i=1}^{n} r_i x_i, f \right\rangle = \sum_i r_i \langle x_i, f \rangle.$$

بخصوص، به‌ازای $(j = 1,2,\ldots,n)$ $f = f_{x_j}$ ،

$$0 = \sum_i r_i\langle x_i, f_{x_j}\rangle = \sum_i r_i\delta_{ij} = r_j.$$

بنابراین $a = \sum_i r_i x_i = \sum_i 0x_i = 0$ ، و θ تکریختی می‌باشد.

(سه) هرگاه X پایه‌ای متناهی از A باشد، آنگاه، طبق قضیهٔ ۱۱۰۴، A^* بر پایهٔ دوگان (متناهی) $\{f_x \mid x \in X\}$ آزاد است. به همین نحو، A^{**} بر پایهٔ دوگان (متناهی) $\{g_x \mid x \in X\}$ آزاد است، که در آن همریختی $g_x : A^* \to R$ به‌ازای هر $x \in X$ با شرط $(y \in X)$ $g_x(f_y) = \delta_{xy}$ به‌طور منحصر به فرد معین می‌شود. اما $\theta(x) \in A^{**}$ یک همریختی $A^* \to R$ است به‌طوری‌که به‌ازای هر $y \in X$

$$\theta(x)(f_y) = \langle x, f_y\rangle = \delta_{xy} = g_x(f_y).$$

از اینرو، $g_x = \theta(x)$ و $\{\theta(x) \mid x \in X\}$ پایه‌ای از A^{**} است. این ایجاب می‌کند که $\operatorname{Im}\theta = A^{**}$. و درنتیجه، θ بروریختی می‌باشد.

تمرینات

تذکر. R حلقه است.

۱. (آ) به‌ازای هر گروه آبلی A و عدد صحیح مثبت m،

$$\operatorname{Hom}(Z_m, A) \cong A[m] = \{a \in A \mid ma = 0\}.$$

(ب) $\operatorname{Hom}(Z_m, Z_n) \cong Z_{(m,n)}$.

(پ) برای $\mathbf{Z}$ ــ مدول Z_m داریم $Z_m{}^* = 0$.

(ت) به‌ازای هر $k \geq 1$، Z_m یک Z_{mk} ــ مدول است (تمرین ۱۰۱)؛ به عنوان یک Z_{mk} ــ مدول، $Z_m{}^* \cong Z_m$.

۲. هرگاه A,B گروههایی آبلی بوده و m,n اعدادی صحیح باشند به‌طوری‌که $mA = 0 = nB$، آنگاه مرتبهٔ هر عنصر $\operatorname{Hom}(A,B)$ ، (m,n) را عاد می‌کند.

۳. فرض کنید $\pi : \mathbf{Z} \to Z_2$ بروریختی کانونی باشد. نگاشت القایی $\bar{\pi} : \operatorname{Hom}(Z_2,\mathbf{Z}) \to \operatorname{Hom}(Z_2,Z_2)$ نگاشت صفر است. چون $\operatorname{Hom}(Z_2,Z_2) \neq 0$ (تمرین ۱ (ب))، $\bar{\pi}$ بروریختی نخواهد بود.

۴. فرض کنید R,S حلقه بوده و $A_R, {}_sB_R, {}_sC_R, D_R$ (دو) مدولهای مربوطه باشند.

همچنین، Hom_R تمام همریختیهای R ــ مدولهای **راست** باشد.

(آ) $\mathrm{Hom}_R(A,B)$ یک S ــ مدول‌چپ است، که عمل S با $(sf)(a) = s(f(a))$ داده می‌شود.

(ب) هرگاه $\varphi : A \to A'$ یک همریختی R ــ مدولهای راست باشد، آنگاه نگاشت القایی $\bar{\varphi} : \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B)$ یک همریختی از S ــ مدولهای چپ است.

(پ) $\mathrm{Hom}_R(C,D)$ یک S ــ مدول‌راست‌است، که عمل S با $(gs)(c) = g(sc)$ داده می‌شود.

(ت) هرگاه $\psi : D \to D'$ یک همریختی R ــ مدولهای راست باشد، آنگاه $\bar{\psi} : \mathrm{Hom}_R(C,D) \to \mathrm{Hom}_R(C,D')$ یک همریختی S ــ مدولهای راست است.

۵. فرض کنید R حلقه‌ای یکدار باشد؛ در این صورت، یک یکریختی **حلقه‌ها** مانند $\mathrm{Hom}_R(R,R) \cong R^{op}$ وجوددارد، که‌درآن Hom_R مبین همریختیهای R ــ مدولهای چپ است (ر.ک. تمرینات III ۱۷۰۱۰ و ۷۰۱). بخصوص، هرگاه R تعویضپذیر باشد، آنگاه یک یکریختی حلقه‌ها مانند $\mathrm{Hom}_R(R,R) \cong R$ وجود خواهد داشت.

۶. فرض کنید S یک زیرمجموعهٔ ناتهی از فضای برداری V روی حلقهٔ بخشی باشد. **صفرساز** S زیرمجموعه‌ای از V^* مانند S^0 است که با ازای هر $s \in S$، $S^0 = \{ f \in V^* \mid \langle s,f \rangle = 0 \}$ داده می‌شود.

(آ) $0^0 = V^*; V^0 = 0; S \neq \{0\} \Rightarrow S^0 \neq V^*$.

(ب) هرگاه W زیرفضایی از V باشد، آنگاه W^0 زیرفضایی از V^* است.

(پ) هرگاه W زیرفضایی از V بوده و $\dim V$ متناهی باشد، آنگاه $\dim W^0 = \dim V - \dim W$.

(ت) فرض کنید W,V همانندر (پ) باشند. در این صورت، یک یکریختی‌مانند $W^* \cong V^*/W^0$ وجود دارد.

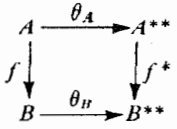
(ث) فرض کنید W,V همانند در (پ)باشند.V را با V^{**} تحت یکریختی θ ی قضیهٔ ۱۲۰۴ یکی کنید. در این صورت، $(W^0)^0 = W \subset V^{**}$.

۷. هرگاه V یک فضای برداری روی حلقهٔ بخشی بوده، $f \in V^*$، و $W = \{a \in V \mid \langle a,f \rangle = 0\}$، آنگاه W زیرفضایی از V می‌باشد. اگر $\dim V$ متناهی باشد، $\dim W$ چقدر است؟

۸. هرگاه R یکدار بوده‌و R ــ مدول چپ R را با ${}_RR$ و R ــ مدول راست R را با

R_R نشان دهیم ، آنگاه $R_R \cong {}_R(R)^* \cong {}_RR$ و $(R_R)^* \cong {}_RR$.

۹ . به‌ازای هر همریختی $f : A \to B$ از R ــ مدولها ، نمودار



تعویضپذیر است ، که در آن θ_A, θ_B همانند در قضیهٔ ۱۲.۴ بوده و f^* نگاشت القا شده بر $A^{**} = \mathrm{Hom}_R(\mathrm{Hom}_R(A,R),R)$ به وسیلهٔ نگاشت $\bar{f} : \mathrm{Hom}_R(B,R) \to \mathrm{Hom}_R(A,R)$ است .

۱۰ . فرض کنید $F = \sum_{x \in X} \mathbf{Z}x$ یک $\mathbf{Z}$ ــ مدول آزاد با پایهٔ نامتناهی X باشد . در این صورت ، $\{f_x \mid x \in X\}$ (قضیهٔ ۱۱.۴) یک پایهٔ F^* را تشکیل نمی‌دهد .

راهنمایی . بنابرقضایای ۷.۴ و ۹.۴ ، $F^* \cong \prod_{x \in X} \mathbf{Z}x$ ؛ اما ، تحت این یکریختی ،

$$f_u \mapsto \{\delta_{xu}x\} \in \prod_{x \in X} \mathbf{Z}x \quad [۱۰$$

تذکر . $F^* = \prod \mathbf{Z}x$ یک $\mathbf{Z}$ ــ مدول آزاد نیست ؛ ر.ک. ال. فوکس [۱۳] ؛ ص ۱۶۸ .

۱۱ . هرگاه R یکدار بوده و P یک R ــ مدول چپ یکانی ، تصویری ، و با تولید متناهی باشد ، آنگاه

(آ) P^* یک R ــ مدول راست تصویری و با تولید متناهی است ؛

(ب) P منعکس است .

این حکم در صورت حذف "با تولید متناهی" ممکن است نادرست باشد ؛ ر.ک. تمرین ۱۰ .

۱۲ . فرض کنید F یک میدان ، X یک مجموعهٔ نامتناهی ، و V ، F ــ مدول چپ آزاد (فضای‌برداری) روی X باشد . همچنین ، F^X مجموعهٔ تمام توابع $f : X \to F$ باشد .

(آ) F^X یک فضای برداری (راست) روی F (با $(f+g)(x) = f(x) + g(x)$ و

$(fr)(x) = rf(x)$) است.

(ب) یک یکریختی فضاهای برداری مانند $V^* \cong F^X$ وجود دارد.

(پ) $\dim_F F^X = |F|^{|X|}$ (ر.ک. آشنایی، تمرین ۱۰۰۸).

(ت) $\dim_F V^* > \dim_F V$ [**راهنمایی.** بنابرآشنایی، تمرین ۱۰۰۸ و آشنایی، قضیهٔ ۱۰۰۵ $\dim_F V^* = \dim_F F^X = |F|^{|X|} \geq 2^{|X|} = |P(X)| > |X| = \dim_F V$].

۵ ضربهای تانسوری

حاصلضرب تانسوری $A \otimes_R B$ مدولهای A_R و $_RB$ روی حلقهٔ R یک گروه آبلی است، که نقش مهمی در بررسی جبر چند خطی دارد. تصور حاصلضرب تانسوری $A \otimes_R B$ به‌عنوان یک شیء عمومی در یک رسته اغلب مفید است (قضیهٔ ۲۰۵). از آن سو، نیز شایسته است $A \otimes_R B$ را به نوعی مفهوم دوگان $\mathrm{Hom}_R(A,B)$ بگیریم. این کار را خواهیم کرد و همچنین مباحثی مانند نگاشتهای القایی و ساختارهای مدولی برای $A_S \otimes_R B$ و نیز رفتار حاصلضربهای تانسوری نسبت به دنباله‌های کامل و مجموعه‌های مستقیم را درنظر خواهیم گرفت.

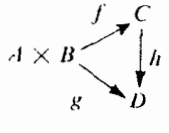
هرگاه A_R و $_RB$ مدولهایی روی حلقهٔ R بوده و C یک گروه آبلی (جمعی) باشد، آنگاه یک **نگاشت خطی میانی** از $A \times B$ به C تابعی است مانند $f : A \times B \to C$ به‌طوری که به‌ازای هر $a, a_i \in A$، $b, b_i \in B$، و $r \in R$،

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b); \tag{۳}$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2); \tag{۴}$$

$$f(ar, b) = f(a, rb). \tag{۵}$$

به‌ازای $A_R, {}_RB$ ثابت، رستهٔ $\mathfrak{M}(A,B)$ را درنظر می‌گیریم که اشیاء آن تمام نگاشتهای خطی میانی بر $A \times B$ اند. طبق تعریف، ریخت در $\mathfrak{M}(A,B)$ از نگاشت خطی میانی $f : A \times B \to C$ به نگاشت خطی میانی $g : A \times B \to D$ یک همریختی گروهها مانند $h : C \to D$ است به‌طوری که نمودار



تعویضپذیر می‌باشد. تحقیق کنید که $\mathfrak{M}(A,B)$ یک رسته است، 1_f ریخت همانی از f به f است، و h یک تعادل در $\mathfrak{M}(A,B)$ است اگر و فقط اگر h یک یکریختی گروهها باشد.

در قضیهٔ ۲۰۵ یک‌شیٔ عمومی در رستهٔ $\mathfrak{M}(A,B)$ خواهیم ساخت (ر.ک. تعریف ۹۰۷۰ i). اما ابتدا به تعریف زیر نیاز داریم.

تعریف ۱۰۵. فرض کنیم A یک مدول راست و B یک‌مدول چپ روی حلقهٔ R باشد. همچنین، F گروه آبلی آزاد بر مجموعهٔ $A \times B$ باشد. و نیز K زیرگروه F تولید شده به وسیلهٔ تمام عناصر به اشکال زیر (به‌ازای هر $a,a' \in A; b,b' \in B; r \in R$) باشد:

(یک) $(a + a',b) - (a,b) - (a',b)$;

(دو) $(a,b + b') - (a,b) - (a,b')$;

(سه) $(ar,b) - (a,rb)$.

گروه خارج قسمتی F/K **حاصل‌ضرب تانسوری** A و B نام دارد؛ این گروه با $A \otimes_R B$ (یا فقط $A \otimes B$ اگر $R = \mathbf{Z}$) نموده‌می‌شود. هم مجموعهٔ $K + (a,b)$ عنصر (a,b) در F با $a \otimes b$ نموده می‌شود؛ هم مجموعهٔ (0,0) با 0 نشان داده خواهد شد.

چون F با مجموعهٔ $A \times B$ تولید شده‌است، گروه خارج‌قسمتی $F/K = A \otimes_R B$ به وسیلهٔ تمام عناصر (هم‌مجموعه‌ها) به شکل $a \otimes b$ $(a \in A, b \in B)$ تولید می‌شود. اما درست **نیست** که هر عنصر $A \otimes_R B$ به شکل $a \otimes b$ است (تمرین ۴). زیرا عنصر نوعی F **مجموع** $\sum_{i=1}^{r} n_i(a_i,b_i)$ $(n_i \in \mathbf{Z}, a_i \in A, b_i \in B)$ است؛ و درنتیجه، هم‌مجموعهٔ آن در $A \otimes_R B = F/K$ به شکل $\sum_{i=1}^{r} n_i(a_i \otimes b_i)$ می‌باشد. به علاوه، چون انتخاب نماینده‌های مختلف برای هم مجموعه امکان دارد، ممکن است در $A \otimes_R B$ داشته باشیم $a \otimes b = a' \otimes b'$ ولی $a \neq a'$ و $b \neq b'$ (تمرین ۴). همچنین، ممکن است، حتی اگر $A \neq 0$ و $B \neq 0$، داشته باشیم $A \otimes_R B = 0$ (تمرین ۳).

تعریف ۱۰۵ ایجاب می‌کند که مولدهای $a \otimes b$ از $A \otimes_R B$ (به‌ازای هر $a,a_i \in A$، $b,b_i \in B$، و $r \in R$) در روابط زیر صدق کنند:

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b; \tag{۶}$$

$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2; \tag{۷}$$

$$ar \otimes b = a \otimes rb. \tag{۸}$$

اثبات این مطالب سرراست است؛ مثلاً، چون $(a_1 + a_2,b) - (a_1,b) - (a_2,b) \in K$،

یعنی "هم‌مجموعهٔ صفر"، داریم

$$[(a_1 + a_2, b) + K] - [(a_1, b) + K] - [(a_2, b) + K] = K;$$

یا، با نماد $(a,b) + K = a \otimes b$،

$$(a_1 + a_2) \otimes b - a_1 \otimes b - a_2 \otimes b = 0.$$

درواقع، تعریف دیگری از $A \otimes_R B$ این است که این گروهی آبلی است که مولدهایش تمام علایم $a \otimes b$ $(a \in A, b \in B)$ اند که در روابط (۶) تا (۸) فوق صدق می‌کنند. به علاوه، چون 0 تنها عنصر یک گروه است که در $x + x = x$ صدق می‌کند، به آسانی معلوم می‌شود که به‌ازای هر $a \in A, b \in B$،

$$a \otimes 0 = 0 \otimes b = 0 \otimes 0 = 0.$$

اگر مدولهای A_R و ${}_RB$ روی حلقهٔ R داده شده باشند، به‌آسانی تحقیق می‌شود که نگاشت $i : A \times B \to A \otimes_R B$ داده شده با $(a,b) \mapsto a \otimes b$ یک نگاشت خطی میانی است. نگاشت i **نگاشت خطی میانی کانونی** نام دارد. اهمیت آن در قضیهٔ زیر دیده می‌شود.

قضیهٔ ۲۰۵. *فرض کنیم A_R و ${}_RB$ مدولهایی روی حلقهٔ R بوده، و C یک گروه آبلی باشد. هرگاه $g : A \times B \to C$ یک نگاشت خطی میانی باشد، آنگاه یک همریختی منحصر به فرد از گروهها مانند $\bar{g} : A \otimes_R B \to C$ وجود دارد به‌طوری‌که $\bar{g}i = g$، که در آن $i : A \times B \to A \otimes_R B$ نگاشت خطی میانی کانونی است. این خاصیت $A \otimes_R B$ را با تقریب یکریختی به‌طور منحصربه‌فرد معین می‌کند. به‌عبارت دیگر، $i : A \times B \to A \otimes_R B$ در رستهٔ $\mathfrak{M}(A,B)$ مرکب از تمام نگاشتهای خطی میانی بر $A \times B$ عمومی است.*

طرح برهان. فرض کنیم F گروه آبلی آزاد بر مجموعهٔ $A \times B$ بوده، و K زیرگروه توصیف شده در تعریف ۱۰۵ باشد. چون F آزاد است، بنابر قضیهٔ ۱۰۲ (چهار)، انتساب $(a,b) \mapsto g(a,b) \in C$ همریختی منحصربه‌فرد $g_1 : F \to C$ را معین می‌کند. با استفاده از اینکه g خطی‌میانی است، نشان دهید که g_1 هر مولد K را به 0 می‌نگارد. از اینرو، $K \subset \operatorname{Ker} g_1$. بنابر قضیهٔ ۷۰۱، g_1 همریختی $\bar{g} : F/K \to C$ را القا می‌کند به‌طوری‌که $\bar{g}[(a,b) + K] = g_1[(a,b)] = g(a,b)$. اما $F/K = A \otimes_R B$ و $(a,b) + K = a \otimes b$. بنابراین، $\bar{g} : A \otimes_R B \to C$ یک همریختی است به‌طوری‌که به‌ازای هر $(a,b) \in A \times B$، $\bar{g}i(a,b) = \bar{g}(a \otimes b) = g(a,b)$؛ یعنی، $\bar{g}i = g$. هرگاه $h : A \otimes_R B \to C$ یک همریختی با

خاصیت $hi = g$ باشد، آنگاه، به‌ازای هر مولد $a \otimes b$ از $A \otimes_R B$،

$$h(a \otimes b) = hi(a,b) = g(a,b) = \bar{g}i(a,b) = \bar{g}(a \otimes b).$$

چون h و $\bar{g}$ همریختیهایی می‌باشند که بر مولدهای $A \otimes_R B$ یکی هستند، باید داشته باشیم $h = \bar{g}$، که از آنجا $\bar{g}$ منحصر به فرد می‌باشد. این ثابت می‌کند که $i : A \times B \to A \otimes_R B$ یک شیء عمومی در رسته‌ٔ تمام نگاشتهای خطی میانی بر $A \times B$ است، که از آنجا $A \otimes_R B$ به وسیلهٔ قضیهٔ I ۱۰۷۰ با تقریب (تعادل) یکریختی به‌طور منحصر به فرد معین می‌شود.

نتیجهٔ ۳۰۵. *هرگاه* A_R، $A_{R'}$، ${}_RB$، و ${}_{R'}B'$ *مدولهایی روی حلقهٔ* R *بوده و* $f : A \to A', g : B \to B'$ *همریختیهایی از* R *ـ مدولها باشند، آنگاه یک همریختی منحصر به فرد از گروهها مانند* $A \otimes_R B \to A' \otimes_R B'$ *وجود دارد به‌طوری‌که به‌ازای هر* $a \in A, b \in B$، $a \otimes b \mapsto f(a) \otimes g(b)$.

طرح برهان. تحقیق کنید که انتساب $(a,b) \mapsto f(a) \otimes g(b)$ نگاشت خطی میانی $h : A \times B \to C = A' \otimes_R B'$ را تعریف می‌کند. بنابر قضیهٔ ۲۰۵، همریختی منحصر به فردی مانند $\bar{h} : A \otimes_R B \to A' \otimes_R B'$ وجود دارد به‌طوری‌که به‌ازای هر $a \in A, b \in B$،

$$\bar{h}(a \otimes b) = \bar{h}i(a,b) = h(a,b) = f(a) \otimes g(b).$$

همریختی منحصربه‌فرد نتیجهٔ ۳۰۵ با $f \otimes g : A \otimes_R B \to A' \otimes_R B'$ نموده می‌شود. هرگاه $f' : A_{R'} \to A_{R''}$ و $g' : {}_RB' \to {}_RB''$ نیز همریختیهای R ـ مدولها باشند، آنگاه به آسانی تحقیق می‌شود که

$$(f' \otimes g')(f \otimes g) = (f'f \otimes g'g) : A \otimes_R B \to A'' \otimes_R B''.$$

بی‌درنگ نتیجه می‌شود که هرگاه f و g یکریختی R ـ مدولها باشند، آنگاه $f \otimes g$ یک یکریختی گروهها با معکوس $f^{-1} \otimes g^{-1}$ است.

حکم ۴۰۵. *هرگاه* $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *یک دنبالهٔ کامل از مدولهای چپ روی حلقهٔ* R *بوده و* D *یک* R *ـ مدول راست باشد، آنگاه*

$$D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \to 0$$

یک دنبالهٔ کامل از گروههای آبلی است. حکم مشابه برای یک دنبالهٔ کامل نسبت به متغیر اول نیز برقرار است.

برهان. باید ثابت کنیم: (یک) $\operatorname{Im}(1_D \otimes g) = D \otimes_R C$؛ (دو) $\operatorname{Im}(1_D \otimes f) \subset \operatorname{Ker}(1_D \otimes g)$؛ (سه) $\operatorname{Ker}(1_D \otimes g) \subset \operatorname{Im}(1_D \otimes f)$.

(یک) چون طبق فرض g بروریختی است، هر مولد $d \otimes c$ از $D \otimes_R C$ به شکل $d \otimes g(b) = (1_D \otimes g)(d \otimes b)$ به‌ازای $b \in B$ ای می‌باشد. لذا، $\operatorname{Im}(1_D \otimes g)$ شامل تمام مولدهای $D \otimes_R C$ است، که از آنجا $\operatorname{Im}(1_D \otimes g) = D \otimes_R C$. (دو) چون $\operatorname{Ker} g = \operatorname{Im} f$، داریم $gf = 0$ و $(1_D \otimes g)(1_D \otimes f) = 1_D \otimes gf = 1_D \otimes 0 = 0$، که از آنجا $\operatorname{Im}(1_D \otimes f) \subset \operatorname{Ker}(1_D \otimes g)$. (سه) فرض‌کنیم

$$\pi : D \otimes_R B \to (D \otimes_R B)/\operatorname{Im}(1_D \otimes f)$$

بروریختی کانونی باشد. بنابر (دو) و قضیهٔ ۷۰۱، یک همریختی مانند $\alpha : (D \otimes_R B)/\operatorname{Im}(1_D \otimes f) \to D \otimes_R C$ موجود است که

$$\alpha(\pi(d \otimes b)) = (1_D \otimes g)(d \otimes b) = d \otimes g(b).$$

نشان‌می‌دهیم‌که α یک یکریختی است. این امر و قضیهٔ ۷۰۱ ایجاب می‌کنند که $\operatorname{Ker}(1_D \otimes g) = \operatorname{Im}(1_D \otimes f)$؛ و لذا، برهان تمام است.

ابتدا نشان می‌دهیم که نگاشت $\beta : D \times C \to (D \otimes_R B)/\operatorname{Im}(1_D \otimes f)$ داده شده با $(d,c) \mapsto \pi(d \otimes b)$، که در آن $g(b) = c$، از انتخاب b مستقل است. توجه کنید که دست‌کم یک چنین b وجود دارد، زیرا g بروریختی است. هرگاه $g(b') = c$، آنگاه $g(b - b') = 0$ و $b - b' \in \operatorname{Ker} g = \operatorname{Im} f$، که‌ازآنجا، به‌ازای $a \in A$ ای، $b - b' = f(a)$. چون $d \otimes f(a) \in \operatorname{Im}(1_D \otimes f)$ و $\pi(d \otimes f(a)) = 0$، داریم

$$\begin{aligned}\pi(d \otimes b) &= \pi(d \otimes b' + f(a)) = \pi(d \otimes b' + d \otimes f(a)) \\ &= \pi(d \otimes b') + \pi(d \otimes f(a)) = \pi(d \otimes b').\end{aligned}$$

بنابراین، β تعریف شده است. تحقیق کنید که β خطی میانی است. در این صورت، طبق قضیهٔ ۲۰۵، همریختی منحصر به فرد $\bar{\beta} : D \otimes_R C \to (D \otimes_R B)/\operatorname{Im}(1_D \otimes f)$ وجود دارد به‌طوری که

$$\bar{\beta}(d \otimes c) = \bar{\beta} i(d,c) = \beta(d,c) = \pi(d \otimes b),$$

که در آن $g(b) = c$. بنابراین، به‌ازای هر مولد $d \otimes c$ از $D \otimes_R C$،

$\alpha\bar{\beta}(d \otimes c) = \alpha(\pi(d \otimes b)) = d \otimes g(b) = d \otimes c$ ، که از آنجا $\alpha\bar{\beta}$ نگاشت همانی است . به همین نحو ، $\bar{\beta}\alpha$ همانی است ؛ درنتیجه ، α یکریختی می‌باشد .

چند تبصره . هرگاه $h : A_R \to A_R'$ و $k : {}_RB \to {}_RB'$ بروریختیهای مدولها باشند ، آنگاه حکم ۴.۵ ایجاب می‌کند که $1_A \otimes k$ و $h \otimes 1_B$ بروریختیهای گروهها هستند . از اینرو ، $h \otimes k = (1_{A'} \otimes k)(h \otimes 1_B)$ بروریختی است ، زیرا $h \otimes k : A \otimes_R B \to A' \otimes_R B'$. اما ، اگر h و k تکریختی باشند ، لازم **نیست** $1_A \otimes k$ و $h \otimes 1_B$ تکریختی باشند (تمرین ۷) .

قضیهٔ ۵.۵ . *فرض کنیم* R و S *حلقه‌بوده و* ${}_SA_R, {}_RB, C_R, {}_RD_S$ *(دو) مدولهای مربوطه باشند .*

(یک) $A \otimes_R B$ *یک* S *ـ مدول چپ است به‌طوری‌که به‌ازای هر* $s \in S, a \in A, b \in B$ ،

$s(a \otimes b) = sa \otimes b$.

(دو) هرگاه $f : A \to A'$ *یک همریختی* S-R *دومدولهابوده و* $g : B \to B'$ *یک همریختی* R *ـ مدولها باشد ، آنگاه نگاشت القایی* $f \otimes g : A \otimes_R B \to A' \otimes_R B'$ *یک همریختی از* S *ـ مدولهای چپ است .*

(سه) $C \otimes_R D$ *یک* S *ـ مدول راست است به‌طوری که به‌ازای هر* $c \in C, d \in D, s \in S$ ،

$(c \otimes d)s = c \otimes ds$.

(چهار) هرگاه $h : C \to C'$ *یک همریختی* R *ـ مدولها بوده و* $k : D \to D'$ *یک همریختی* R-S *دو مدولها باشد ، آنگاه نگاشت القایی* $h \otimes k : C \otimes_R D \to C' \otimes_R D'$ *یک همریختی* S *ـ مدولهای راست است .*

طرح برهان . (یک) به‌ازای هر $s \in S$ ، نگاشت $A \times B \to A \otimes_R B$ داده شده با $(a,b) \mapsto sa \otimes b$ یک‌خطی میانی R ـ مدولهاست ؛ ولذا ، همریختی منحصر به فردی ازگروهها مانند $\alpha_s : A \otimes_R B \to A \otimes_R B$ را القا می‌کند به‌طوری‌که $\alpha_s(a \otimes b) = sa \otimes b$. به‌ازای هر عنصر $u = \sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_R B$ ، su را عنصر $\alpha_s(u) = \sum_{i=1}^{n} \alpha_s(a_i \otimes b_i) = \sum_{i=1}^{n} sa_i \otimes b_i$ تعریف می‌کنیم . چون α_s همریختی است ، این عمل S تعریف شده است (یعنی ، مستقل از نگارش u به صورت مجموعی از مولدهاست) . حال به آسانی تحقیق می‌شود که $A \otimes_R B$ یک S ـ مدول چپ است .

تبصره. حالت خاص مهمی از قضیهٔ ۵.۵ وقتی رخ می‌دهد که R یک حلقهٔ تعویضپذیر است؛ ودرنتیجه، هر R ــ مدول A یک R-R دو مدول با خاصیت $ra = ar$ $(r \in R, a \in A)$ می‌باشد. در این حالت، $A \otimes_R B$ نیز یک R-R دو مدول است، که به‌ازای هر $r \in R, a \in A, b \in B$،

$$r(a \otimes b) = ra \otimes b = ar \otimes b = a \otimes rb = a \otimes br = (a \otimes b)r.$$

هرگاه R حلقه‌ای تعویضپذیر باشد، آنگاه حاصلضرب تانسوری R ــ مدولها را می‌توان بـا صورت مفیدی از قضیهٔ ۲.۵ توصیف کرد. فرض کنیم A,B,C مدولهایی روی حلقهٔ تعویضپذیر R باشند. **نگاشت دو خطی** از $A \times B$ به C تابعی است مانند $f : A \times B \to C$ به‌طوری‌که به‌ازای هر $a,a_i \in A$، $b,b_i \in B$، و $r \in R$،

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b); \tag{۹}$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2); \tag{۱۰}$$

$$f(ra, b) = rf(a, b) = f(a, rb). \tag{۱۱}$$

شرایط (۹) و (۱۰) صرفاً بیانهای دیگری از (۳) و (۴)اند. برای مدولهای روی یک حلقهٔ تعویضپذیر، رابطهٔ (۱۱) بوضوح شرط (۵) فوق را ایجاب می‌کند؛ درنتیجه، هر نگاشت دوخطی،خطی میانی می‌باشد.

مثال. هرگاه A^* دوگان مدول A روی حلقهٔ تعویضپذیر R باشد، آنگاه نگاشت $A \times A^* \to R$ داده شده با $(a,f) \mapsto f(a) = \langle a,f \rangle$ دو خطی است (ر.ک. ص ۳۱۷).

مثال. هرگاه A و B مدولهایی روی حلقهٔ تعویضپذیر R باشند، آنگاه $A \otimes_R B$ نیز چنین‌است و به‌آسانی دیده می‌شود که نگاشت خطی میانی کانونی $i : A \times B \to A \otimes_R B$ دو خطی است. در این محدوده، i **نگاشت دو خطی کانونی** نام دارد.

قضیهٔ ۶.۵. *هرگاه A,B,C مدولهایی روی حلقهٔ تعویضپذیر R بوده و $g : A \times B \to C$ یک نگاشت دوخطی باشد، آنگاه همریختی R ــ مدولهای منحصر به فردی مانند $\bar{g} : A \otimes_R B \to C$ وجوددارد به‌طوری‌که $\bar{g}i = g$، که در آن $i : A \times B \to A \otimes_R B$ نگاشت دوخطی کانونی است. این خاصیت مدول $A \otimes_R B$ را با تقریب یکریختی به‌طور منحصر*

به فرد معین می‌کند.

طرح برهان. تحقیق کنید که همریختی منحصر به فرد $\bar{g}: A \otimes_R B \to C$ از گروههای آبلی داده شده با قضیهٔ ۲۰۵ عملاً یک همریختی R ــ مدولهاست. برای اثبات آخرین حکم، فرض کنیم $\mathfrak{B}(A,B)$ رستهٔ تمام نگاشتهای دوخطی بر $A \times B$ باشد (که به وسیلهٔ تعویض گروههای C,D و همریختی گروههای $h: C \to D$ با مدولها و همریختیهای مدولها در تعریف $\mathfrak{M}(A,B)$ در صفحهٔ ۳۲۳ تعریف می‌شود). در این صورت، قسمت اول قضیه نشان می‌دهد که $i: A \times B \to A \otimes_R B$ یک شیٔ عمومی در $\mathfrak{B}(A,B)$ است، که از آنجا $A \otimes_R B$ به وسیلهٔ قضیهٔ I ۷۰.۱۰ با تقریب یکریختی به‌طور منحصر به فرد معین می‌شود.

قضیهٔ ۶۰۵ را نیز می‌توان برای به دست آوردن تعریفی دیگر از $A \otimes_R B$، وقتی R حلقه‌ای تعویضپذیر و یکدار است، به کار برد. فرض کنیم F_1، R ــ **مدول** آزاد بر مجموعهٔ $A \times B$ بوده و K_1 **زیرمدول** تولید شده به وسیلهٔ تمام عناصر به اشکال

$$(a + a',b) - (a,b) - (a',b);$$
$$(a,b + b') - (a,b) - (a,b');$$
$$(ra,b) - r(a,b);$$
$$(a,rb) - r(a,b);$$

باشند، که در آنها $a,a' \in A$، $b,b' \in B$، و $r \in R$ (با تعریف ۱۰۵ مقایسه کنید). حکم می‌کنیم که یک یکریختی R ــ مدولها مانند $A \otimes_R B \cong F_1/K_1$ وجود دارد. مشابه بدیهی برهان قضیهٔ ۲۰۵ نشان می‌دهد که نگاشت $A \times B \to F_1/K_1$ داده‌شده با $(a,b) \mapsto 1_R(a,b) + K_1$ یک شیٔ عمومی در رستهٔ $\mathfrak{B}(A,B)$ از نگاشتهای دو خطی بر $A \times B$ است. درنتیجه، بنابر قضیهٔ ۶۰۵، $A \otimes_R B \cong F_1/K_1$.

حال به مدولها روی حلقه‌های دلخواه بازمی‌گردیم.

قضیهٔ ۷۰۵. *هرگاه* R *حلقه‌ای یکدار بوده و* $A_{R,\ R}B$ ــ *مدولهای یکانی باشند، آنگاه یکریختیهای* R*-مدولهای زیر وجود دارند:*

$$A \otimes_R R \cong A \quad \text{و} \quad R \otimes_R B \cong B.$$

طرح برهان. چون R یک R-R دو مدول است، بنابر قضیهٔ ۵۰۵، $R \otimes_R B$ یک

R ــ مدول چپ است. انتساب $(r,b)\mapsto rb$ یک نگاشت خطی میانی مانند $R\times B\to B$ را تعریف می‌کند. بنابر قضیهٔ ۲۰۵، یک همریختی گروهها مانند $\alpha: R\otimes_R B\to B$ وجود دارد به‌طوری‌که $\alpha(r\otimes b)=rb$. تحقیق کنید که α درواقع یک همریختی R ــ مدول‌های چپ است. سپس تحقیق کنید که نگاشت $\beta: B\to R\otimes_R B$ داده شده با $b\mapsto 1_R\otimes b$ یک‌یکریختی R-مدولهاست به‌طوری‌که $\alpha\beta=1_B$ و $\beta\alpha=1_{R\otimes_R B}$. ازاینرو، $R\otimes_R B\cong B$، $\alpha: R\otimes_R B\cong B$. یکریختی $A\otimes_R R\cong A$ به همین نحو ساخته می‌شود.

هرگاه R و S حلقه و $A_R, {}_RB_S, {}_SC$ دو (مدول) باشند، آنگاه بنابر قضیهٔ ۵۰۵، $A\otimes_R B$، S ــ مدول راست و $B\otimes_S C$، R ــ مدول چپ است. درنتیجه، هر دوی $(A\otimes_R B)\otimes_S C$ و $A\otimes_R (B\otimes_S C)$ گروههای آبلی تعریف شده‌ای هستند.

قضیهٔ ۸۰۵. هرگاه R و S حلقه و $A_R, {}_RB_S, {}_SC$ دو (مدول) باشند، آنگاه یک یکریختی مانند

$$(A\otimes_R B)\otimes_S C\cong A\otimes_R (B\otimes_S C)$$

موجود است.

برهان. طبق تعریف، هر عنصر v از $(A\otimes_R B)\otimes {}_SC$ یک مجموع متناهی مانند $\sum_{i=1}^{n} u_i\otimes c_i$ $(u_i\in A\otimes_R B, c_i\in C)$ است. چون هر $u_i\in A\otimes_R B$ مجموعی متناهی مانند $\sum_{j=1}^{m_i} a_{ij}\otimes b_{ij}$ $(a_{ij}\in A, b_{ij}\in B)$ است، داریم

$$v=\sum_i u_i\otimes c_i=\sum_i\Big(\sum_j a_{ij}\otimes b_{ij}\Big)\otimes c_i=\sum_i\sum_j[(a_{ij}\otimes b_{ij})\otimes c_i].$$

بنابراین، $(A\otimes_R B)\otimes_S C$ به‌وسیلهٔ تمام عناصر به شکل $(a\otimes b)\otimes c$ $(a\in A, b\in B, c\in C)$ تولید می‌شود. به همین نحو، $A\otimes_R (B\otimes_S C)$ به وسیلهٔ تمام $a\otimes(b\otimes c)$ ها تولید می‌شود، که $\Big(\sum_{i=1}^{n} a_i\otimes b_i, c\Big)\mapsto\sum_{i=1}^{n}[a_i\otimes(b_i\otimes c)]$، $a\in A, b\in B, c\in C$، تحقیق کنید که انتساب یک نگاشت خطی S ــ میانی $(A\otimes_R B)\times C\to A\otimes_R (B\otimes_S C)$ تعریف می‌کند. بنابراین،

طبق قضیهٔ ۲۰۵ ، یک همریختی مانند

$$\alpha : (A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$$

وجـود دارد ، کـه به‌ازای هر $a \in A, b \in B, c \in C$ ، $\alpha[(a \otimes b) \otimes c] = a \otimes (b \otimes c)$. به همین‌نحو ، یک نگاشت خطی R ــ میانی مانند $A \times (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ وجود دارد که همریختی

$$\beta : A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$$

را القامی‌کند به‌طوری‌که به‌ازای هر $a \in A, b \in B, c \in C$ ، $\beta[a \otimes (b \otimes c)] = (a \otimes b) \otimes c$. به‌ازای هر مولد $(a \otimes b) \otimes c$ از $(A \otimes_R B) \otimes_S C$ ، $\beta\alpha[(a \otimes b) \otimes c] = (a \otimes b) \otimes c$ ، کـه از آنجـا نگاشت همانی بر $(A \otimes_R B) \otimes_S C$ می‌بـاشد . استدلالی مشابه نشان می‌دهد که $\beta\alpha$ بر $A \otimes_R (B \otimes_S C)$ همانی است . لذا ، α و β یکریختی می‌باشند .

در آینده $(A \otimes_R B) \otimes_S C$ و $A \otimes_R (B \otimes_S C)$ را تحت یکـریختی قضیهٔ ۸۰۵ یکی کرده و فقط می‌نویسیم $A \otimes_R B \otimes_S C$. حال می‌توان حاصلضرب تانسوری n تایی

$$A^1 \otimes_{R_1} A^2 \otimes_{R_2} \cdots \otimes_{R_n} A^{n+1}$$

را به‌طور بازگشتی تعریف کرد ، که در آن $R_1, \ldots, R_n$ حلقه و $A_{R_1}{}^1{}_{,R_1}A_{R_2}{}^2, \ldots, {}_{R_n}A^{n+1}$ دو (مدول) بـاشند . یـک چنین حاصلضربهای تانسوری مکرر رامی‌توان برحسب نگاشتهای n ــ خطی عمومی توصیف کرد (تمرین ۱۰) .

قضیهٔ ۹۰۵ . *فـرض کنیـم R حلقه ، A و $\{A_i \mid i \in I\}$ ، R ــ مدولهایی راست ، و B و $\{B_j \mid j \in J\}$ ، R ــ مدولهایی چپ باشند . در این صورت ، یکریختیهای*

$$(\sum_{i \in I} A_i) \otimes_R B \cong \sum_{i \in I} (A_i \otimes_R B);$$
$$A \otimes_R (\sum_{j \in J} B_j) \cong \sum_{j \in J} (A \otimes_R B_j)$$

از گروهها وجود دارند .

برهان . فرض کنیم ι_k, π_k انژکسیونها و تصاویر کانونی $\sum_{i \in I} A_i$ باشند . بنابر قضیهٔ ۵۰۸۰ I ، خـانوادهٔ همـریختیهای $\iota_k \otimes 1_B : A_k \otimes_R B \to (\sum_{i \in I} A_i) \otimes_R B$ وجود دارند که همریختی

$\alpha : \sum_{i\in I}(A_i \otimes_R B) \to (\sum_{i\in I} A_i) \otimes_R B$ را القا کنند به‌طوری‌که

$$\alpha[\{a_i \otimes b\}] = \sum_{i\in I_0}(\iota_i(a_i) \otimes b) = (\sum_{i\in I_0} \iota_i(a_i)) \otimes b,$$

که در آن $I_0 = \{i \in I \mid a_i \otimes b \neq 0\}$. انتساب $(u,b) \mapsto \{\pi_i(u) \otimes b\}_{i\in I}$ یک نگاشت خطی میانی مانند $(\sum_{i\in I} A_i) \times B \to \sum_{i\in I}(A_i \otimes_R B)$ تعریف می‌کند؛ و لذا، همریختی $\beta : (\sum A_i) \otimes_R B \to \sum (A_i \otimes_R B)$ القا می‌شود به‌طوری‌که $\beta(u \otimes b) = \{\pi_i(u) \otimes b\}_{i\in I}$. نشان می‌دهیم که $\alpha\beta$ و $\beta\alpha$ نگاشتهایی همانی‌اند، که از آنجا α یک یکریختی است.

به یاد آورید که هرگاه $u \in \sum A_i$ و $I_0 = \{i \in I \mid \pi_i(u) \neq 0\}$، آنگاه $u = \sum_{i\in I_0} \iota_i\pi_i(u)$. لذا، به‌ازای هر مولد $u \otimes b$ از $(\sum A_i) \otimes_R B$ ، داریم

$$\alpha\beta(u \otimes b) = \alpha[\{\pi_i(u) \otimes b\}] = (\sum_{i\in I_0} \iota_i\pi_i(u)) \otimes b = u \otimes b.$$

درنتیجه، $\alpha\beta$ نگاشت همانی می‌باشد.

به‌ازای هر $j \in I$ ، فرض کنید $\iota_j^* : A_j \otimes {}_RB \to \sum_i (A_i \otimes_R B)$ انژکسیون کانونی باشد و تحقیق کنید که $\sum_i (A_i \otimes_R B)$ به وسیلهٔ تمام عناصر به شکل $\iota_j^*(a \otimes b) = \{\pi_i\iota_j(a) \otimes b\}_{i\in I}$ $(j \in I, a \in A_j, b \in B)$ تولید می‌شود. به‌ازای هر چنین مولد داریم $(\pi_i\iota_j(a)) \otimes b = 0$ اگر $i \neq j$ و $(\pi_j\iota_j(a)) \otimes b = a \otimes b$ ، که از آنجا

$$\begin{aligned}\beta\alpha[\iota_j^*(a \otimes b)] &= \beta\alpha[\{\pi_i\iota_j(a) \otimes b\}] = \beta[\iota_j\pi_j\iota_j(a) \otimes b] \\ &= \beta[\iota_j(a) \otimes b] = \{\pi_i\iota_j(a) \otimes b\}_{i\in I} = \iota_j^*(a \otimes b).\end{aligned}$$

درنتیجه، نگاشت $\beta\alpha$ باید همانی باشد. یکریختی دوم به همین نحو ثابت می‌شود.

قضیهٔ ۱۰.۵ (شرکتپذیری الحاقی). *فرض کنیم R و S حلقه بوده و $A_{R,\,R}B_S,\ C_S$ (دو) مدول باشند. در این صورت، یک یکریختی از گروههای آبلی مانند*

$$\alpha : Hom_S(A \otimes_R B, C) \cong Hom_R(A, Hom_S(B,C))$$

وجود دارد که به‌ازای هر $f : A \otimes_R B \to C$ با

$$[(\alpha f)(a)](b) = f(a \otimes b)$$

تعریف می‌شود .

توجه کنید که $\mathrm{Hom}_R(\_,\_)$ و $\mathrm{Hom}_S(\_,\_)$ از همریختیهای مدولهای *راست* تشکیل شده‌اند . به یاد آورید که ساختار R ــ مدولی $\mathrm{Hom}_S(B,C)$ با $(gr)(b) = g(rb)$ (به‌ازای $r \in R,\ b \in B,\ g \in \mathrm{Hom}_S(B,C)$ ؛ ر . ک . تمرین ۴.۴ (پ)) داده شده است .

طرح برهان ۱۰.۵ . برهان تمرین سرراستی در استفاده از تعاریف مناسب است . موارد زیر باید امتحان شوند .

(یک) به‌ازای هر $a \in A$ و $f \in \mathrm{Hom}_S(A \otimes_R B,C)$ ، $(\alpha f)(a) : B \to C$ یک همریختی S ــ مدولهااست .

(دو) $(\alpha f) : A \to \mathrm{Hom}_S(B,C)$ یک همریختی R ــ مدولهاست . لذا ، α یک‌تابع تعریف شده است .

(سه) α یک همریختی گروههاست (یعنی ، $\alpha(f_1 + f_2) = \alpha(f_1) + \alpha(f_2)$). برای نشان دادن‌اینکه α یکریختی‌است ، نگاشت‌معکوس $\beta : \mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C)) \to \mathrm{Hom}_S(A \otimes_R B,C)$ را با تعریف

$$(\beta g)(a \otimes b) = [g(a)](b)$$

می‌سازیم ، که در آن $a \in A$ ، $b \in B$ ، و $g \in \mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C))$. تحقیق کنید که (چهار) βg به صورت تعریف شده در بالا بر مولدها ، همریختی منحصر به فرد S ــ مدولهایی مانند $A \otimes_R B \to C$ را معین می‌کند .

(پنج) β همریختی است .

(شش) $\beta\alpha$ و $\alpha\beta$ همانی می‌باشند . لذا ، α یکریختی می‌باشد .

این بخش را با بررسی حاصلضرب تانسوری مدولهای آزاد به پایان می‌بریم . این مطالب ، جز گهگاه در یک تمرین ، فقط در بخش IX . ۶ به کار خواهند رفت .

قضیهٔ ۱۱.۵ . *فرض کنیم* R *حلقه‌ای یکدار باشد . هرگاه* A *یک* R ــ *مدول راست یکانی‌بوده و* F *یک* R ــ *مدول‌چپ‌آزاد با پایهٔ* Y *باشد ، آنگاه هر عنصر* u *از* $A \otimes_R F$

را می‌توان به‌طور منحصر به فرد به شکل $u = \sum_{i=1}^{n} a_i \otimes y_i$ نوشت، که در آن $a_i \in A$ و y_i عناصر متمایز Y اند.

تبصره. اگر $u = \sum_{k=1}^{t} a_k \otimes y_k$ و $v = \sum_{j=1}^{m} b_j \otimes z_j$ ($a_k, b_i \in A, y_k, z_i \in Y$)، می‌توان، در صورت لزوم، جملاتی به شکل $0 \otimes y$ ($y \in Y$) را درج و فرض کرد $u = \sum_{i=1}^{n} a_i \otimes y_i$ و $v = \sum_{i=1}^{n} b_i \otimes y_i$. کلمهٔ "به‌طور منحصر به فرد" در قضیهٔ ۱۱۰۵ یعنی هرگاه $\sum_{i=1}^{n} a_i \otimes y_i = \sum_{i=1}^{n} b_i \otimes y_i$، آنگاه، به‌ازای هر i، $a_i = b_i$. بخصوص، هرگاه $\sum_{i=1}^{n} a_i \otimes y_i = 0 = \sum_{i=1}^{n} 0 \otimes y_i$، آنگاه، به‌ازای هر i، $a_i = 0$.

برهان ۱۱۰۵. به‌ازای هر $y \in Y$، فرض کنیم A_y یک نسخه از A بوده و مجموع مستقیم $\sum_{y \in Y} A_y$ را در نظر می‌گیریم. ابتدا یکریختی $\theta : A \otimes_R F \cong \sum_{y \in Y} A_y$ را به‌صورت زیر می‌سازیم. چون Y پایه است، $\{y\}$ به‌ازای هر $y \in Y$ مجموعه‌ای مستقل خطی می‌باشد. درنتیجه، بروریختی R ــ مدولهای $\varphi : R \to Ry$ داده شده با $r \mapsto ry$ (قضیهٔ ۵۰۱) درواقع یک یکریختی است. بنابراین، طبق قضیهٔ ۷۰۵، به‌ازای هر $y \in Y$ یک یکریختی مانند

$$A \otimes_R Ry \xrightarrow{1_A \otimes \varphi^{-1}} A \otimes_R R \cong A = A_y$$

وجود دارد. لذا، طبق قضایای ۹۰۵ و I ۱۱۰۸۰، یک یکریختی مانند θ وجود دارد:

$$A \otimes_R F = A \otimes_R (\sum_{y \in Y} Ry) \cong \sum_{y \in Y} A \otimes_R Ry \cong \sum_{y \in Y} A_y.$$

تحقیق کنید که به‌ازای هر $a \in A, z \in Y$، $\theta(a \otimes z) = \{u_y\} \in \sum A_y$، که در آن $u_z = a$ و، به‌ازای $y \neq z$، $u_y = 0$؛ به عبارت دیگر، $\theta(a \otimes z) = \iota_z(a)$، که در آن $\iota_z : A_z \to \sum A_y$ انژکسیون کانونی می‌باشد. اما هر $v \in \sum A_y$ ناصفر مجموعی متناهی چون

$y_1, \ldots, y_n$ است ، که در آن $v = \iota_{v_1}(a_1) + \cdots + \iota_{v_n}(a_n) = \theta(a_1 \otimes y_1) + \cdots + \theta(a_n \otimes y_n)$ عناصر متمایزی از Y بوده و a_i ها عناصر ناصفر به‌طور منحصر به فرد معین شدهٔ A می‌باشند . پس نتیجه‌می‌شود که هر عنصر $A \otimes_R F$ (که لزوما " به‌ازای v ای مساوی $\theta^{-1}(v)$ است) را می‌توان به‌طور منحصر به فرد به صورت $\sum_{i=1}^{n} a_i \otimes y_i$ نوشت .

نتیجهٔ ۱۲۰۵ . ***هرگاه R حلقه‌ای یکدار بوده و A_R و $_RB$ ، R ــ مدولهایی آزاد به ترتیب با پایه‌های X و Y باشند ، آنگاه $A \otimes_R B$ یک R ــ مدول (راست) آزاد با پایهٔ $W = \{x \otimes y \mid x \in X, y \in Y\}$ به اصلیت $|X||Y|$ می‌باشد .***

چند تبصره . چون R یک R-R دو مدول است ، هر مجموع مستقیم از نسخه‌های R چنین‌اند . بخصوص، هر R ــ مدول چپ آزاد نیز یک R ــ مدول راست آزاد است و بالعکس. با اینحال ، کلا " درست نیست که یک R ــ مدول (چپ) آزاد یک شیٔ آزاد در رستهٔ R-R دو مدولها باشد (تمرین ۱۲) .

طرح برهان ۱۲۰۵ . بنابربرهان‌قضیهٔ ۱۱۰۵ وقضیهٔ ۱۰۲ (برای R ــ مدولهای‌راست) ، یک یکریختی گروهها مانند

$$v : A \otimes_R B \cong \sum_{y \in Y} A_y = \sum_{y \in Y} A = \sum_{y \in Y} (\sum_{x \in X} xR)$$

وجود دارد . چون طبق تبصرهٔ پیش از برهان ، B یک R-R دو مدول است ، $A \otimes_R B$ ، طبق قضیهٔ ۵۰۵ ، یک R ــ مدول راست می‌باشد . تحقیق کنید که θ یک یکریختی از R ــ مدولهای‌راست‌است به‌طوری که $\theta(W)$ پایه‌ای از R ــ مدول راست آزاد $\sum_Y (\sum_X xR)$ می‌باشد . بنابراین ، $A \otimes_R B$ یک Rــمدول‌راست آزاد با پایهٔ W می‌باشد . چون عناصر W طبق قضیهٔ ۱۱۰۵ متمایزند ، $|W| = |X||Y|$.

نتیجهٔ ۱۳۰۵ . ***فرض کنیم S حلقه‌ای یکدار بوده و R زیرحلقه‌ای از S شامل 1_S باشد . هرگاه F یک R ــ مدول چپ آزاد با پایهٔ X باشد ، آنگاه $S \otimes_R F$ یک S ــ مدول چپ***

آزاد با پایهٔ $\{1_S \otimes x \mid x \in X\}$ به اصلیت $|X|$ می‌باشد.

طرح برهان. چون S بوضوح یک S-R دو مدول است، طبق قضیهٔ ۵۰۵، $S \otimes_R F$ یک Sـ مدول‌چپ‌است. برهان قضیهٔ ۱۱۰۵ نشان می‌دهد که یک یکریختی گروهها مانند $\theta : S \otimes_R F \cong \sum_{x \in X} S_x$ وجوددارد، که درآن هر $S_x = S$. به علاوه، هرگاه به‌ازای $z \in X$، $\iota_z : S = S_z \to \sum_{x \in X} S_x$ انژکسیون‌کانونی‌باشد، آنگاه، به‌ازای‌هر $z \in X$، $\theta(1_S \otimes z) = \iota_z(1_S)$. تحقیق کنید که θ عملا" یک‌یکریختی Sـ مدولهای‌چپ‌است. واضح است که $\{\iota_x(1_S) \mid x \in X\}$ یک پایه به اصلیت $|X|$ از S ـ مدول چپ آزاد $\sum_{x \in X} S_x$ است، که از آنجا $S \otimes_R F$ یک S ـ مدول آزاد با پایهٔ $\{1_S \otimes x \mid x \in X\}$ به اصلیت $|X|$ می‌باشد.

تمرینات

تذکر. R حلقه است و $\otimes = \otimes_{\mathbf{Z}}$.

۱. هرگاه $R = \mathbf{Z}$، آنگاه شرط (سه) تعریف ۱۰۵ زاید است (یعنی، (یک) و (دو) شرط (سه) را ایجاب می‌کنند).

۲. فرض‌کنید A و B گروههایی آبلی باشند.

(آ) به‌ازای هر $m > 0$، $A \otimes Z_m \cong A/mA$.

(ب) $Z_m \otimes Z_n \cong Z_c$، که در آن $c = (m,n)$.

(پ) $A \otimes B$ را درصورتی توصیف کنید که A و B با تولید متناهی باشند.

۳. هرگاه A یک گروه آبلی تابی و $\mathbf{Q}$ گروه (جمعی) اعداد گویا باشد، آنگاه

(آ) $A \otimes \mathbf{Q} = 0$؛

(ب) $\mathbf{Q} \otimes \mathbf{Q} \cong \mathbf{Q}$.

۴. با مثال نشان دهید که هر یک از روابط زیر به ازای حلقهٔ R و مدولهای $A_R, {}_RB$ مناسب برقرار است:

(آ) $A \otimes_R B \neq A \otimes_{\mathbf{Z}} B$؛

(ب) $u \in A \otimes_R B$ ولی، به‌ازای هر $a \in A, b \in B$، $u \neq a \otimes b$.

(پ) $a \otimes b = a_1 \otimes b_1$ ولی $a \neq a_1$ و $b \neq b_1$.

۵. هرگاه A' یک زیرمدول R ـ مدول راست A بوده و B' زیرمدول R ـ مدول چپ

B باشد ، آنگاه $A/A' \otimes_R B/B' \cong (A \otimes_R B)/C$ ، که در آن C زیرگروه $A \otimes_R B$ است که بـه وسیلهٔ تمـام عناصر $a' \otimes b$ و $a \otimes b'$ کـه $a \in A, a' \in A', b \in B, b' \in B'$ تولید می‌شود .

۶ . فرض کنید $f : A_R \to A_R'$ و $g : {}_RB \to {}_RB'$ همریختیهای R ــ مدولها باشند . تفاوت بیـن همـریختی $f \otimes g$ (به صورت داده شـده با نتیجهٔ ۳۰۵) و عنصر $f \otimes g$ حاصلضرب تانسوری گروههای آبلی

$$\mathrm{Hom}_R(A,A') \otimes \mathrm{Hom}_R(B,B')$$

چیست ؟

۷ . انژکسیون معمولی $\alpha : Z_2 \to Z_4$ یک تکـریختی گروههای آبلی است . نشان دهید که $1 \otimes \alpha : Z_2 \otimes Z_2 \to Z_2 \otimes Z_4$ نگاشت صفر است (ولی $Z_2 \otimes Z_2 \neq 0$ و $Z_2 \otimes Z_4 \neq 0$ ؛ ر.ک. تمرین ۲) .

۸ . فرض کنید $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ دنبالهٔ کامل کوتاه از R-مدولهای چپ بوده و D یک R ــ مدول راست باشد . در این صورت، $0 \to D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \to 0$ یک دنبالهٔ کامل کوتاه از گروههای آبلی تحت یکی از فرضهای زیر است :

(آ) $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ کامل تجزیه است .

(ب) R یکدار بوده و D یک R ــ مدول راست آزاد است .

(پ) R یکدار بوده و D یک R ــ مدول راست یکانی‌تصویری است .

۹ . (آ) هرگاه I یک ایده‌آل راست حلقهٔ یکدار R و B یک R ــ مدول چپ باشد ، آنگاه یک همریختی گروهها مانند $R/I \otimes_R B \cong B/IB$ وجود دارد ، که در آن IB زیرگروهی از B است که به وسیلهٔ تمام عناصر rb که $r \in I, b \in B$ تولید می‌شود .

(ب) هرگاه R تعویضپذیربوده‌و I,J ایده‌آلهایی از R باشند ، آنگاه یک یکریختی R ــ مدولها مانند $R/I \otimes_R R/J \cong R/(I+J)$ وجود خواهد داشت .

۱۰ . اگر R,S حلقه ، $A_R, {}_RB_S, {}_SC$ (دو) مدولها ،و D گروهی آبلی باشد ، **نگاشت خطی میانی** را تابعی تعریف کنید مانند $f : A \times B \times C \to D$ به‌طوری که

(یک) $f(a+a',b,c) = f(a,b,c) + f(a',b,c)$ ؛

(دو) $f(a,b+b',c) = f(a,b,c) + f(a,b',c)$ ؛

(سه) $f(a,b,c+c') = f(a,b,c) + f(a,b,c')$ ؛

(چهار) به‌ازای $r \in R$ ، $f(ar,b,c) = f(a,rb,c)$ ؛

(پنج) به‌ازای $s \in S$ ، $f(a,bs,c) = f(a,b,sc)$.

(آ) نگاشت $i : A \times B \times C \to (A \otimes_R B) \otimes_S C$ داده شده با $(a,b,c) \mapsto (a \otimes b) \otimes c$ خطی میانی است.

(ب) نگاشت خطی میانی i **عمومی** است؛ یعنی، به‌ازای نگاشت خطی میانی $g : A \times B \times C \to D$ ، یک همریختی منحصر به فرد از گروهها مانند $\bar{g} : (A \otimes_R B) \otimes_S C \to D$ وجود دارد به‌طوری که $\bar{g}i = g$.

(پ) نگاشت $j : A \times B \times C \to A \otimes_R (B \otimes_S C)$ داده شده با $(a,b,c) \mapsto a \otimes (b \otimes c)$ نیز یک نگاشت خطی میانی عمومی می‌باشد.

(ت) بنابر قسمتهای (ب) ، (پ) ، و قضیهٔ I ۱۰.۷۰ ،

$$(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C) .$$

(ث) تابع خطی میانی بر n (دو) مدول $(n \geq 4)$ را به طرز روشنی تعریف کرده و برهان تعمیم نتایج بالا را به حالت (دو) مدول (روی $n-1$ حلقه) به‌اختصار بیان نمایید.

(ج) اگر $R = S$ ، R تعویضپذیر بوده و A,B,C,D ، R ــ مدول باشند، نگاشت سه خطی $A \times B \times C \to D$ را تعریف‌کرده و نتایج (آ) ، (ب) ، و (پ) را به این گونه نگاشتها تعمیم دهید.

۱۱ . فرض کنید A,B,C مدولهایی روی حلقهٔ تعویضپذیر R باشند.

(آ) مجموعهٔ $\mathfrak{L}(A,B;C)$ متشکل از تمام نگاشتهای R ــ دو خطی $A \times B \to C$ یک R ــ مدول است، که در آن $(f+g)(a,b) = f(a,b) + g(a,b)$ و $(rf)(a,b) = rf(a,b)$.

(ب) هر یک از R ــ مدولهای زیر با $\mathfrak{L}(A,B;C)$ یکریخت است:

(یک) $\mathrm{Hom}_R(A \otimes_R B, C)$ ؛

(دو) $\mathrm{Hom}_R(A, \mathrm{Hom}_R(B,C))$ ؛

(سه) $\mathrm{Hom}_R(B, \mathrm{Hom}_R(A,C))$.

۱۲ . فرض کنید R یکدار باشد. همچنین، $\mathfrak{C}$ رستهٔ تمام R-R دو مدولهای یکانی و همریختیهای دو مدولی (یعنی، همریختیهای گروهها مانند $f : A \to B$ به‌طوری‌که به‌ازای هر $r,s \in R$ ، $f(ras) = rf(a)s$) باشد. فرض کنید $X = \{1_R\}$ و $\iota : X \to R$ نگاشت شمول باشد.

(آ) هرگاه R غیرتعویضپذیرباشد، آنگاه R (مجهز به $\iota: X \to R$) یک شیٔ آزاد بر مجموعهٔ X در رستهٔ $\mathcal{C}$ نیست.

(ب) $R \otimes_{\mathbb{Z}} R$ یک R-R دو مدول است (قضیهٔ ۵۰۵). هرگاه $\iota: X \to R \otimes_{\mathbb{Z}} R$ با $1_R \mapsto 1_R \otimes 1_R$ دادهشده باشد، آنگاه $R \otimes_{\mathbb{Z}} R$ یک شیٔ آزاد بر مجموعهٔ X در رستهٔ $\mathcal{C}$ است.

۶ مدولها روی دامنهٔ ایدهآل اصلی

هدف اصلی این بخش، که فقط در بخشهای VII ۲۰ و VII ۴۰ به کار خواهد رفت، تعیین ساختار تمام مدولهای با تولید متناهی روی دامنهٔ ایدهآل اصلی است. اساساً تمام قضایای ساختاری در باب گروههای آبلی با تولید متناهی (بخشهای II ۱۰ و II ۲۰) به این گونه مدولها سرایت میکنند. درواقع، بسیاری از برهانها در بخشهای II ۱۰ و II ۲۰ بیدرنگ به مدولها روی دامنههای اقلیدسی تعمیم مییابند. با اینحال، چندتایی هستند که برای برقراری در مورد مدولها روی یک دامنهٔ ایدهآل اصلی دلخواه بایدتبدیل بسیار بیابند. درنتیجه، برای اثبات قضایای ساختاری در اینجا از روش متفاوتی استفاده میکنیم. نشان میدهیم که، مثل گروههای آبلی، هر مدول باتولید متناهی را میتوان بهدو راه به مجموع مستقیمی از زیرمدولهای دوری تجزیه کرد (قضیهٔ ۱۲۰۶). هر تجزیه مجموعهای از پایاها را برای مدول داده شده فراهم میسازد (یعنی، دو مدول دارای پایاهای یکسانند اگر و فقط اگر یکریخت باشند (نتیجهٔ ۱۳۰۶)). لذا، هر روش تجزیه به ردهبندی کاملی (با تقریب یکریختی) از تمام مدولها با تولید متناهی روی دامنهٔ ایدهآل اصلی منجر میشود. *اینجا و سراسر این بخش "مدول" یعنی "مدول یکانی".*

با مدولهای آزادروی دامنهٔ ایدهآل اصلی R آغاز میکنیم. چون R، طبق نتیجهٔ ۱۲۰۲، خاصیت بعد پایا دارد، رتبهٔ یک R ــ مدول آزاد (تعریف ۸۰۲) تعریف شده است. بخصوص، دو R ــ مدول آزاد یکریختاند اگر و فقط اگر هر دو یک رتبه داشته باشند (حکم ۹۰۲). به علاوه، تعمیم زیر از قضیهٔ II ۱۰۶ را خواهیم داشت.

قضیهٔ ۱۰۶. *فرض کنیم F یک مدول آزاد روی دامنهٔ ایدهآل اصلی R بوده و G زیر مدول F باشد. در این صورت، G یک R ــ مدول آزاد بوده و $\operatorname{rank} G \leq \operatorname{rank} F$.*

طرح برهان. فرض کنیم $\{x_i \mid i \in I\}$ پایه‌ای از F باشد. در این صورت، $F = \sum_{i \in I} Rx_i$، که در آن هر Rx_i با R (به عنوان یک R ــ مدول چپ) یکریخت است. مجموعهٔ I را با $\leq$ خوش ترتیب می‌کنیم (آشنایی، بخش ۷). به‌ازای هر $i \in I$، تالی بلافصل i را با $i+1$ نشان می‌دهیم (مقدمه، تمرین ۷۰۷). فرض کنیم $J = I \cup \{\alpha\}$، که در آن $\alpha \notin I$ و، طبق تعریف، به‌ازای هر $i \in I$، $i < \alpha$. دراین صورت، J خوش ترتیب است و هر عنصر I تالی بلافصل‌در J دارد.[1] به‌ازای‌هر $j \in J$، F_j، رازیرمدولی از F تعریف کنید که به وسیلهٔ مجموعهٔ $\{x_i \mid i < j\}$ تولید می‌شود. تحقیق کنید که زیرمدولهای F_j از خواص زیر برخوردارند:

(یک) $j < k \Leftrightarrow F_j \subset F_k$؛

(دو) $\bigcup_{j \in J} F_j = F$؛

(سه) به‌ازای هر $i \in I$، $F_{i+1}/F_i \cong Rx_i \cong R$. [قضیهٔ ۷۰۱ را در مورد تصویر کانونی $F_{i+1} = \sum_{k<i+1} Rx_k \to Rx_i$ اعمال کنید.]

به‌ازای هر $j \in J$، فرض کنید $G_j = G \cap F_j$ و تحقیق کنید که

(چهار) $j < k \Rightarrow G_j \subset G_k$؛

(پنج) $\bigcup_{j \in J} G_j = G$؛

(شش) به‌ازای هر $i \in I$، $G_i = G_{i+1} \cap F_i$.

خاصیت (شش) و قضیهٔ ۹۰۱ (یک) ایجاب می‌کنند که

$$G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \cong (G_{i+1} + F_i)/F_i$$

اما $(G_{i+1} + F_i)/F_i$ زیر مدول F_{i+1}/F_i است. بنابراین، G_{i+1}/G_i طبق (سه) با زیرمدولی از R یکریخت‌است. اما هر زیرمدول R لزوما" ایده‌آلی از R است؛ و درنتیجه، به شکل $(c) = Rc$ به‌ازای $c \in R$ ای می‌باشد. هرگاه $c \neq 0$، آنگاه برویختی $R \to Rc$ ــ مدولهای قضیهٔ ۵۰۱ (یک) عملا" یکریختی است. لذا، هر زیرمدول R (و درنتیجه، هر G_{i+1}/G_i) آزاد از مرتبهٔ 0 یا 1 می‌باشد. بنابر قضایای ۲۰۳ و ۴۰۳، دنبالهٔ

---

۱. مجموعهٔ I در طرح تکنیکی لازم برای مقابله با این امکان است که عنصری (لزوما" منحصر به فرد) از I تالی بلافصل در I ندارد. این مثلا "وقتی I متناهی است رخ می‌دهد.

$0 \to G_i \subseteq G_{i+1} \to G_{i+1}/G_i \to 0$ به‌ازای هر $i \in I$ کامل تجزیه است. قضیهٔ ۱۸۰۱ و تمرین ۱۵۰۱ ایجاب می‌کنند که هر G_{i+1} یک مجموع مستقیم داخلی $G_i \oplus Rb_i$ باشد، که $G_{i+1} = G_i \oplus Rb_i$ و $Rb_i \cong R$ اگر $G_{i+1} \neq G_i$، و $b_i = 0$ اگر $G_{i+1} = G_i$ (یعنی، $b_i \in G_{i+1} - G_i$ در آن $G_{i+1}/G_i = 0$). لذا، $b_i \in G$ به‌ازای هر $i \in I$ تعریف شده است. فرض کنیم $B = \{b_i \mid b_i \neq 0\}$. در این صورت $|B| \leq |I| = \operatorname{rank} F$. برای اتمام برهان، کافی است نشان دهیم B یک پایهٔ G است.

فرض کنیم $u = \sum_j r_j b_j = 0$ ($j \in I$ ؛ $r_j \in R$ ؛ مجموع متناهی). همچنین، k بزرگترین اندیس (در صورت وجود یکی) باشد به‌طوری‌که $r_k \neq 0$. در این صورت، $u = \sum_{j<k} r_j b_j + r_k b_k \in G_k \oplus Rb_k = G_{k+1}$، که $r_k = 0$ ایجاب می‌کند. اما $u = 0$ که یک تناقض است. از اینرو، به‌ازای هر j، $r_j = 0$. بنابراین، B مستقل خطی است.

بالاخره، باید ثابت کنیم B، G را می‌پیماید. طبق (پنج) کافی است ثابت کنیم به‌ازای هر $k \in J$، زیرمجموعهٔ $B_k = \{b_i \in B \mid j < k\}$ از B، G_k را می‌پیماید. از استقرای ترانسفینی استفاده می‌کنیم (آشنایی، قضیهٔ ۱۰۷). بنابراین، فرض کنیم B_j، G_j را به‌ازای $j < k$ بپیماید و $u \in G_k$. هرگاه به‌ازای $j \in I$ ای، $k = j + 1$، آنگاه $G_k = G_{j+1} = G_j \oplus Rb_j$ و $u = v + rb_j$ که در آن $v \in G_j$. طبق فرض استقرا، v مجموعی متناهی مانند $v = \sum r_i b_i$ است، که در آن $r_i \in R$ و $b_i \in B_j \subset B_k$. بنابراین، $u = \sum r_i b_i + rb_k$، که از آنجا B_k، G_k را تولید می‌کند. حال فرض کنیم به‌ازای هر $j \in I$، $k \neq j + 1$ (و این ممکن است رخ دهد؛ ر.ک. امثلهٔ پیش از قضیهٔ ۱۰۷ در آشنایی). چون $u \in G_k = G \cap F_k$، u مجموعی متناهی چون $u = \sum r_i x_i$ است، که در آن $j < k$. هرگاه t بزرگترین اندیس باشد به‌طوری که $r_t \neq 0$، آنگاه $u \in F_{t+1}$ که، طبق فرض، $t + 1 < k$. بنابراین، $u \in G \cap F_{t+1} = G_{t+1}$، که در آن $t + 1 < k$. طبق فرض استقرا، u ترکیبی خطی از عناصر B_{t+1} است که زیرمجموعه‌ای از B_k می‌باشد. از اینرو، B_k، G_k را می‌پیماید.

نتیجهٔ ۲۰۶. *فرض کنیم R یک دامنهٔ ایده‌آل اصلی باشد. هرگاه A یک R ــ مدول با تولید متناهی به وسیلهٔ n عنصر باشد، آنگاه هر زیرمدول A را می‌توان با n_1 عنصر*

که $m \leq n$ تولید کرد .

برهان . تمرین ؛ ر.ک. نتیجهٔ II ۷.۱۰ و نتیجهٔ ۲.۲ .

نتیجهٔ ۳.۶ . *مدول یکانی A روی دامنهٔ ایده‌آل اصلی آزاد است اگر و فقط اگر تصویری باشد .*

برهان . ($\Leftarrow$) قضیهٔ ۲.۳ . ($\Rightarrow$) یک دنبالهٔ کامل کوتاه مانند $0 \to K \subseteq F \xrightarrow{f} A \to 0$ وجود دارد که در آن ، بنابر نتیجهٔ ۲.۲ ، F آزاد است ، f بروریختی است ، و $K = \ker f$. هرگاه A تصویری باشد ، آنگاه ، طبق قضیهٔ ۴.۳ ، $F \cong K \oplus A$. بنابراین ، A با زیرمدول F یکریخت است ، که از آنجا ، طبق قضیهٔ ۱.۶ ، A آزاد می‌باشد .

حال مشابه‌های مرتبهٔ یک عنصر در یک گروه و زیرگروه تابی یک گروه آبلی را بیان می‌کنیم .

قضیهٔ ۴.۶ . *فرض کنیم A یک مدول چپ روی دامنهٔ صحیح R بوده و ، به‌ازای هر $a \in A$ ، $\mathcal{O}_a = \{r \in R \mid ra = 0\}$.*

(یک) به‌ازای هر $a \in A$ ، $\mathcal{O}_a$ ایده‌آلی از R است .

(دو) $A_t = \{a \in A \mid \mathcal{O}_a \neq 0\}$ زیرمدولی از A است .

(سه) به‌ازای هر $a \in A$ ، یک یکریختی از مدولهای چپ مانند

$$R/\mathcal{O}_a \cong Ra = \{ra \mid r \in R\}$$

وجود دارد .

فرض کنیم R یک دامنهٔ ایده‌آل اصلی و $p \in R$ اول باشد .

(چهار) هرگاه $p^i a = 0$ (معادلا " ، $(p^i) \subset \mathcal{O}_a$)، آنگاه $\mathcal{O}_a = (p^j)$ ، که در آن $0 \leq j \leq i$.

(پنج) هرگاه $\mathcal{O}_a = (p^j)$ ، آنگاه به‌ازای هر j که $0 \leq j < i$ ، $p^j a \neq 0$.

تبصره . بنابر قضیهٔ III ۴.۳۰ ، عناصر اول و تحویل‌ناپذیر در دامنهٔ ایده‌آل اصلی یکی هستند .

طرح برهان ۴۰۶. (سه) از قضایای ۵۰۱ (یک) و ۷۰۱ استفاده کنید. (چهار) طبق فرض، به‌ازای $r \in R$ ی، $\mathfrak{O}_a = (r)$. چون $p^i \in \mathfrak{O}_a$، r، p^i را عاد می‌کند. یکتایی تجزیه در R (قضیهٔ III ۷۰۳۰) ایجاب می‌کند که $r = p^i u$، که در آن $0 \leq j \leq i$ و یکه‌است. از اینرو، طبق قضیهٔ III ۲۰۳۰، $\mathfrak{O}_a = (r) = (p^i u) = (p^i)$. (پنج) هرگاه $p^i a = 0$ که در آن $j < i$، آنگاه $p^i \in \mathfrak{O}_a = (p^i)$، که‌ازآنجا $p^i | p^i$. این یکتایی تجزیه در R را نقض می‌کند.

فرض کنیم A یک مدول روی یک دامنهٔ صحیح باشد. ایده‌آل $\mathfrak{O}_a$ در قضیهٔ ۴۰۶ را **ایده‌آل مرتبهٔ** $a \in A$ می‌نامند. زیرمدول A_t درقضیهٔ ۴۰۶ **زیرمدول تابی** A نام دارد. گوییم A یک مدول‌تابی‌است اگر $A = A_t$ و **فارغ از تاب**است‌اگر $A_t = 0$. هر مدول آزاد فارغ از تاب است، ولی عکس‌آن درست نیست (تمرین ۲).

فرض‌کنیم A یک مدول روی دامنهٔ ایده‌آل اصلی R باشد. ایده‌آل مرتبهٔ $a \in A$ یک ایده‌آل اصلی R است، مثلا $\mathfrak{O}_a = (r)$، و گوییم a دارای **مرتبهٔ** r است. عنصر r فقط با تقریب ضرب در یکه منحصر به فرد است (قضیهٔ III ۲۰۳۰). زیرمدول دوری Ra که به وسیلهٔ a تولید می‌شود (قضیهٔ ۵۰۱) **دوری از مرتبهٔ** r نام دارد. قضیهٔ ۴۰۶ (سه) نشان می‌دهد که $a \in A$ دارای مرتبهٔ 0 است (یعنی، Ra یک مدول دوری از مرتبهٔ 0 است) اگر و فقط اگر $Ra \cong R$ (یعنی، Ra آزادو از رتبهٔ‌یک‌است). همچنین، $a \in A$ دارای مرتبهٔ r است، که r یکه است، اگر و فقط اگر $a = 0$؛ (زیرا $a = 1_R a = r^{-1}(ra) = r^{-1}0 = 0$).

مثال. هرگاه R دامنهٔ ایده‌آل اصلی بوده و $r \in R$، آنگاه حلقهٔ خارج قسمتی $R/(r)$ یک R ــ مدول دوری با مولد $a = 1_R + (r)$ است. واضح است که $\mathfrak{O}_a = (r)$، که از آنجا a دارای مرتبهٔ r بوده و $R/(r)$ دوری از مرتبهٔ r می‌باشد. قضیهٔ ۴۰۶ (سه) نشان می‌دهد که هر مدول دوری C روی دامنهٔ ایده‌آل اصلی R با $R/(r)$ یکریخت است، که در آن $\mathfrak{O}_a = (r)$ و a مولد C می‌باشد.

مثال. فرض‌کنیم $R = \mathbf{Z}$ و A یک گروه‌آبلی (جمعی) باشد. همچنین، مرتبهٔ نظریهٔ گروههای $a \in A$ به‌عنوان‌عضوی‌ازگروه (تعریف I ۳۰۳۰) متناهی باشد. در این صورت،

$\mathcal{O}_a = (n)$ ، که در آن $|n|$ مرتبهٔ a به عنوان عضوی از گروه است. هرگاه $a \in A$ مرتبهٔ نامتناهی داشته باشد، آنگاه $\mathcal{O}_a = (0)$. در هر حالت، $\mathbf{Z}a$ زیرگروه دوری $\langle a \rangle$ تولید شده به وسیلهٔ a است (قضیهٔ I ۸.۲۰). به علاوه، اگر $\mathcal{O}_a = (n)$، $\mathbf{Z}a \cong \mathbf{Z}/(n) \cong Z_n$ ؛ و $n \neq 0$ اگر $\mathbf{Z}a \cong \mathbf{Z}/(0) \cong \mathbf{Z}$ اگر $\mathcal{O}_a = (0)$.

قضیهٔ ۵.۶. *مدول فارغ از تاب با تولید متناهی A روی دامنهٔ ایده‌آل اصلی R آزاد است.*

تبصره. فرض با تولید متناهی A اساسی است (تمرین II ۱۰.۱۰).

برهان ۵.۶. می‌توان فرض کرد $A \neq 0$. فرض کنیم X مجموعه‌ای متناهی ازمولدهای ناصفر A باشد. هرگاه $x \in X$، آنگاه $rx = 0$ $(r \in R)$ اگروفقط اگر $r = 0$، زیرا A فارغ از تاب است. درنتیجه، زیرمجموعه‌ای ناتهی مانند $S = \{x_1, \ldots, x_k\}$ از X وجود دارد که نسبت به خاصیت زیر ماکزیمال است:

به‌ازای هر i، $r_1x_1 + \cdots + r_kx_k = 0\ (r_i \in R) \Rightarrow r_i = 0$،

واضح است که زیرمدول F تولید شده به وسیلهٔ S یک R ــ مدول آزاد با پایهٔ S است. هرگاه $y \in X - S$، آنگاه، بنابر ماکزیمالی، عناصری مانند $r_0, r_1, \ldots, r_k \in R$ وجود دارند که همه صفر نیستند به‌طوری‌که $r_0y + r_1x_1 + \cdots + r_kx_k = 0$. در این صورت، $r_0y = -\sum_{i=1}^{k} r_ix_i \in F$. به علاوه، $r_0 \neq 0$، زیرا در غیر این صورت، به‌ازای هر i، $r_i = 0$. چون X متناهی است، عنصر ناصفری مانند $r \in R$ (یعنی، $r = \prod_{y \in X - S} r_y$) وجود دارد به‌طوری که $rX = \{rx \mid x \in X\} \subset F$ مشمول F است. بنابراین، $rA = \{ra \mid a \in A\} \subset F$. به آسانی معلوم می‌شود که نگاشت $f : A \to A$ داده شده با $a \mapsto ra$ یک‌همریختی R ــ مدولهابانقش rA است. چون A فارغ‌ازتاب‌است، $\operatorname{Ker} f = 0$، که از آنجا $A \cong \operatorname{Im} f = rA \subset F$. بنابراین، طبق قضیهٔ ۱.۶، A آزاد می‌باشد.

حال تعیین ساختار یک مدول با تولید متناهی A روی دامنهٔ ایده‌آل اصلی در سه

مرحله صورت می‌گیرد. ابتدا نشان می‌دهیم A مجموع مستقیم یک مدول تابی و یک مدول آزاد است (قضیهٔ ۶.۶). هر مدول تابی مجموع مستقیم "مدولهای p ــ اولیه" می‌باشد (قضیهٔ ۷.۶). بالاخره، هر مدول p ــ اولیه مجموع مستقیم مدولهای دوری می‌باشد (قضیهٔ ۹.۶).

قضیهٔ ۶.۶. *هرگاه A یک مدول با تولید متناهی روی دامنهٔ ایده‌آل اصلی R باشد، آنگاه $A = A_t \oplus F$، که در آن F یک R ــ مدول آزاد با رتبهٔ متناهی بوده و $F \cong A/A_t$.*

طرح برهان. مدول خارج‌قسمتی A/A_t فارغ از تاب است، زیرا به‌ازای هر $r \neq 0$،

$$r(a + A_t) = A_t \implies ra \in A_t \implies r_1(ra) = 0 \text{، ی } r_1 \neq 0 \implies a \in A_t$$

به علاوه، A/A_t با تولید متناهی است چون A چنین است. بنابراین، طبق قضیهٔ ۵.۶، A/A_t آزاد و با رتبهٔ متناهی است. درنتیجه، دنبالهٔ کامل $0 \to A_t \subseteq A \to A/A_t \to 0$ کامل تجزیه است. و $A \cong A_t \oplus A/A_t$ (قضایای ۲.۳ و ۴.۳). نقش A_t تحت یکریختی $A \cong A_t \oplus A/A_t$ قضیهٔ ۴.۳، مساوی A_t و نقش A/A_t زیرمدول F از A است، که لزوماً آزاد و با رتبهٔ متناهی است. پس نتیجه می‌شود که A مجموع مستقیم داخلی $A = A_t \oplus F$ است (ر.ک. قضیهٔ ۱۵.۱).

قضیهٔ ۷.۶. *فرض کنیم A یک مدول تابی روی دامنهٔ ایده‌آل اصلی R بوده و، به‌ازای هر $p \in R$ اول، قرار می‌دهیم $A(p) = \{a \in A \mid$ مرتبهٔ a توانی از p است$\}$.*

(یک) به‌ازای هر $p \in R$ اول، $A(p)$ زیرمدولی از A است؛

(دو) $A = \sum A(p)$، که در آن مجموع روی تمام $p \in R$ های اول گرفته شده است. اگر A با تولید متناهی باشد، فقط تعدادی متناهی از $A(p)$ ها ناصفر است.

برهان. (یک) فرض کنیم $a,b \in A(p)$. اگر $\mathcal{O}_a = (p^r)$ و $\mathcal{O}_b = (p^s)$، قرار می‌دهیم $k = \max(r,s)$. در این صورت، $p^k(a+b) = 0$، که از آنجا، بنابر قضیهٔ ۴.۶ (چهار)، $\mathcal{O}_{a+b} = (p^i)$ که $0 \leq i \leq k$. بنابراین، $a,b \in A(p)$ ایجاب می‌کند که استدلالی مشابه نشان می‌دهد که $a \in A(p)$ و $r \in R$ ایجاب می‌کنند که $ra \in A(p)$. بنابراین، $A(p)$ یک زیرمدول می‌باشد.

(دو) فرض کنیم $a \in A$ و $a \neq 0$ که $\mathcal{O}_a = (r)$. بنابر قضیهٔ ۷.۳۰ III ، $r = p_1^{n_1} \cdots p_k^{n_k}$ ، که در آن p_i ها اعداد اول متمایزی در R بوده و هر $n_i > 0$. به‌ازای هر i ، فرض کنیم $r_i = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$. در این صورت ، $r_1, \ldots, r_k$ ها نسبت به هم اول بوده و عناصری مانند $s_1, \ldots, s_k \in R$ وجود دارند به‌طوری‌که $s_1 r_1 + \cdots + s_k r_k = 1_R$ (قضیهٔ ۱۱.۳۰ III) . درنتیجه ، $a = 1_R a = s_1 r_1 a + \cdots + s_k r_k a$. اما $p_i^{n_i} s_i r_i a = s_i r a = 0$ ، که از آنجا $s_i r_i a \in A(p_i)$. ثابت کرده‌ایم که زیرمدولهای $A(p)$ (p اول) مدول A را تولید می‌کنند .

فرض کنیم $p \in R$ اول بوده و A_1 زیرمدولی از A باشد که به وسیلهٔ تمام $A(q)$ ها که $q \neq p$ تولید شود . همچنین ، $a \in A(p) \cap A_1$. در این صورت ، به‌ازای $m \geq 0$ ی ، $p^m a = 0$ و $a = a_1 + \cdots + a_t$ ، که در آن به‌ازای اعداد اولی چون $q_1, \ldots, q_t$ همه متمایز با p ، $a_i \in A(q_i)$. چون $a_i \in A(q_i)$ ، اعداد صحیحی مانند m_i وجود دارند به‌طوری‌که $q_i^{m_i} a_i = 0$ ، که از آنجا $(q_1^{m_1} \cdots q_t^{m_t}) a = 0$. هرگاه $d = q_1^{m_1} \cdots q_t^{m_t}$ ، آنگاه p^m و d نسبت به هم اولند و ، به‌ازای $r, s \in R$ ی ، $rp^m + sd = 1_R$. درنتیجه ، $a = 1_R a = rp^m a + sda = 0$. بنابراین، طبق قضیهٔ ۱۵.۱، $A(p) \cap A_1 = 0$ و $A = \sum A(p)$. آخرین حکم قضیه نتیجه‌ای است از این مطلب آسان به دست آمده که مجموع مستقیم مدولها با تعدادی نامتناهی جمعوند ناصفر را نمی‌توان به‌طور متناهی تولید کرد . زیرا هر مولد فقط تعدادی متناهی مختصات ناصفر دارد .

برای تعیین ساختار مدولهای با تولید متناهی که در آنها هر عنصر مرتبه‌اش توانی از عدد اول p است (نظیر $A(p)$ در قضیهٔ ۷.۶) ، به یک لم نیاز داریم . هرگاه A یک R ــ مدول بوده و $r \in R$ ، آنگاه rA مجموعهٔ $\{ra \mid a \in A\}$ است .

لم ۸.۶ . فرض کنیم A مدولی روی دامنهٔ ایده‌آل اصلی R باشد به‌طوری‌که به‌ازای $p \in R$ ای اول و عدد صحیح مثبت n ، $p^n A = 0$ و $p^{n-1} A \neq 0$. فرض کنیم a عنصری از A با مرتبهٔ p^n باشد .

(یک) هرگاه $Ra \neq A$ ، آنگاه عنصر ناصفری مانند $b \in A$ هست به‌طوری‌که $Ra \cap Rb = 0$.

(دو) زیرمدول C از A وجود دارد به‌طوری‌که $A = Ra \oplus C$.

تبصره. برهان زیر نسبتا" مقدماتی است. برهانی با ظرافت بیشتر از (دو)، که در آن از مفهوم انژکتیوی استفاده می‌شود، در تمرین ۷ داده شده است.

برهان ۸.۰۶. (جی. اس. مونک[1]) (یک) هرگاه $A \neq Ra$، آنگاه $c \in A - Ra$ ای وجود دارد. چون $p^n c \in p^n A = 0$، کوچکترین عدد صحیح **مثبت** j وجود دارد به‌طوری‌که $p^j c \in Ra$، که از آنجا $p^{j-1}c \notin Ra$ و $(r_1 \in R)\ p^j c = r_1 a$. چون R دامنهٔ یکتایی تجزیه است، به‌ازای $k \geq 0$ ای و $r \in R$ که $p \nmid r$، $r_1 = rp^k$. درنتیجه،

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j} r p^k a$$

(قضیهٔ ۴.۰۶ (پنج))، باید $p^{n-1}a \neq 0$ و $p \nmid r$. چون $n - j + k \geq n$، که از آنجا $k \geq j \geq 1$. بنابراین، $b = p^{j-1}c - rp^{k-1}a$ عنصر تعریف شده‌ای از A است. به علاوه، $b \neq 0$ (چون $p^{j-1}c \notin Ra$) و $pb = p^j c - rp^k a = p^j c - r_1 a = 0$. هرگاه $Ra \cap Rb \neq 0$، آنگاه $s \in R$ ی هست به‌طوری که $sb \in Ra$ و $sb \neq 0$. چون $sb \neq 0$ و $pb = 0$، p، s را عاد نمی‌کند. بنابراین، s و p^n نسبت به‌هم اولند و، به‌ازای $x, y \in R$ ی، $sx + p^n y = 1_R$ (قضیهٔ III ۱۱.۰۳۰). لذا، چون $p^n A = 0$، $b = 1_R b = sxb + p^n yb = x(sb) \in Ra$. درنتیجه $p^{j-1}c = b + rp^{k-1}a \in Ra$. اگر $j - 1 \neq 0$، این مینیمالی j را نقض می‌کند، و اگر $j - 1 = 0$، این با $c \notin Ra$ تعارض دارد. بنابراین، $Ra \cap Rb = 0$.

(دو) اگر $A = Ra$، قرار می‌دهیم $C = 0$. هرگاه $A \neq Ra$، آنگاه $\mathcal{S}$ را مجموعهٔ تمام زیرمدولهای B از A می‌گیریم که $Ra \cap B = 0$. $\mathcal{S}$ ناتهی است زیرا، طبق (یک)، عنصر ناصفری مانند $b \in A$ وجود دارد به‌طوری‌که $Ra \cap Rb = 0$. $\mathcal{S}$ را با شمول نظریهٔ مجموعه‌ها جزئی مرتب کرده و تحقیق کنید هر زنجیر در $\mathcal{S}$ دارای کران بالایی در $\mathcal{S}$ است. بنابر لم زرن، زیرمدولی مانند C از A هست که در $\mathcal{S}$ ماکزیمال است. مدول خارج‌قسمتی A/C را درنظر می‌گیریم. واضح است که $p^n(A/C) = 0$ و $p^n(a + C) = 0$. چون $Ra \cap C = 0$ و $p^{n-1}a \neq 0$، داریم $p^{n-1}(a + C) \neq C$، که از آنجا $a + C$ دارای مرتبهٔ p^n در A/C است و $p^{n-1}(A/C) \neq 0$. اما، هرگاه A/C، R ــ مدول دوری تولید شده به وسیلهٔ $a + C$ **نباشد** (یعنی، $A/C \neq R(a + C)$)، آنگاه، بنابر (یک)، عنصری مانند $d + C \in A/C$ وجود دارد به‌طوری‌که $d + C \neq C$ و $R(a + C) \cap R(d + C) = C$.

---

1. G. S. Monk

چون $Ra \cap C = 0$ ، نتیجه می‌شود که $Ra \cap (Rd + C) = 0$. چون $d \notin C$ ، $Rd + C$ در S است و حقیقتاً " شامل C می‌باشد ، که ماکزیمالی C را نقض می‌کند . بنابراین ، A/C ، R ــ مدول‌دوری‌تولیدشده‌به وسیلهٔ $a + C$ است (یعنی ، $A/C = R(a + C)$) . درنتیجه ، $A = Ra + C$ ، که از آنجا ، طبق قضیهٔ ۱۵۰۱ ، $A = Ra \oplus C$.

قضیهٔ ۹۰۶ . فرض کنیم A یک‌مدول‌با‌تولید متناهی روی دامنهٔ ایده‌آل اصلی R باشد به‌طوری‌که‌هرعنصر A مرتبه‌اش توانی‌از $p \in R$ اول باشد در این صورت ، A مجموع مستقیمی از R ـ مدولهای دوری‌به‌ترتیب‌ازمرتبه‌های $p^{n_1}, \ldots, p^{n_k}$ است ،که $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.

برهان . برهان به استقرا بر تعداد r مولدهای A پیش می‌رود ، که در آن حالت $r = 1$ بدیهی است . هرگاه $r > 1$ ، آنگاه A به وسیلهٔ عناصر $a_1, \ldots, a_r$ تولید می‌شود که مرتبه‌های آنها به ترتیب عبارتند از $p^{n_1}, p^{m_2}, p^{m_3}, \ldots, p^{m_r}$. می‌توان فرض کرد

$$n_1 = \max\{n_1, m_2, \ldots, m_r\}$$

پس $p^{n_1}A = 0$ و $p^{n_1-1}A \neq 0$. بنابر لم ۸۰۶ ، زیرمدول C از A وجود دارد به‌طوری‌که $A = Ra_1 \oplus C$. فرض کنیم π برووریختی کانونی $\pi : A \to C$ باشد . چون A به وسیلهٔ $a_1, a_2, \ldots, a_r$ تولید می‌شود ، C باید به وسیلهٔ $\pi(a_1), \pi(a_2), \ldots, \pi(a_r)$ تولید شود . اما $\pi(a_1) = 0$ ؛ درنتیجه ، C را می‌توان با $r - 1$ یا عناصر کمتری تولید کرد . درنتیجه ، فرض استقرا ایجاب می‌کند که C مجموع مستقیمی از R ــ مدولهای دوری به ترتیب از مرتبه‌های $p^{n_2}, p^{n_3}, \ldots, p^{n_k}$ باشد که $n_2 \geq n_3 \geq \cdots \geq n_k \geq 1$. لذا ، C شامل عنصری از مرتبهٔ p^{n_2} است . چون $p^{n_1}A = 0$ ، داریم $p^{n_1}C = 0$ ، که ازآنجا $n_1 \geq n_2$. چون Ra_1 یک R ــ مدول دوری از مرتبهٔ p^{n_1} است ، A مجموع مستقیم R ــ مدولهای دوری به ترتیب از مرتبه‌های $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$ می‌باشد که $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.

قضایای ۶۰۶ ، ۷۰۶ ، و ۹۰۶ بی‌درنگ قضیهٔ ساختاری برای مدولهای با تولید متناهی‌روی‌دامنهٔ‌ایده‌آل اصلی را به دست دهند . (ر.ک. قضیهٔ ۱۲۰۶ (دو) در زیر) . مثل حالت گروههای آبلی (بخش ۲۰ II) ، راه دومی برای تجزیهٔ یک مدول با تولید متناهی‌به‌عنوان‌مجموعی مستقیم از زیرمدولهای دوری وجود دارد . برای به دست آوردن این‌تجزیهٔ‌دوم و اثبات قضیهٔ یکتایی‌درباب هریک‌ازتجزیه‌ها ، به دو لم زیر نیاز داریم .

لم ۱۰.۶ . فرض کنیم A ، B ، و A_i ها $(i \in I)$ مدولهایی روی دامنهٔ ایده‌آل اصلی R باشند . همچنین ، $r \in R$ و $p \in R$ اول باشد .

(یک) $rA = \{ra \mid a \in A\}$ و $A[r] = \{a \in A \mid ra = 0\}$ زیرمدولهایی از A هستند .

(دو) $R/(p)$ میدان بوده و $A[p]$ یک فضای برداری روی $R/(p)$ است .

(سه) به‌ازای هر عدد صحیح مثبت n ، یکریختیهای R ــ مدولهایی مانند

$$(R/(p^n))[p] \cong R/(p) \ , \ p^m(R/(p^n)) \cong R/(p^{n-m}) \ (0 \leq m < n)$$

وجود دارند

(چهار) هرگاه $A \cong \sum_{i \in I} A_i$ ، آنگاه $rA \cong \sum_{i \in I} rA_i$ و $A[r] \cong \sum_{i \in I} A_i[r]$.

(پنج) هرگاه $f : A \to B$ یک یکریختی R ــ مدولها باشد ، آنگاه $f : A_t \cong B_t$ و $f : A(p) \cong B(p)$.

طرح برهان . (دو) تمرین ۴۰۲ . (پنج) ر.ک. لم II ۵۰۲۰ (هفت) . (سه) اولین مثال پیش‌از قضیهٔ ۵۰۶ ممکن است مفید باشد . تحقیق کنید که $(R/(p^n))[p]$ به عنوان یک R ــ مدول (و درنتیجه ، یک فضای برداری روی $R/(p)$) با تنها عنصر ناصفر $p^{n-1} + (p^n)$ تولید می‌شود . بنابراین ، طبق قضایای ۵۰۲ و ۱۰۲ ، $(R/(p^n))[p] \cong R/(p)$. زیرمدول $R/(p^n)$ تولید شده به وسیلهٔ $p^m + (p^n)$ دقیقا " $p^m(R/(p^n))$ است . چون $p^m + (p^n)$ دارای مرتبهٔ p^{n-m} است ، طبق قضیهٔ ۴۰۶ (سه) ، داریم $p^m(R/(p^n)) \cong R/(p^{n-m})$.

لم ۱۱۰۶ . فرض کنیم R دامنهٔ ایده‌آل اصلی باشد . هرگاه $r \in R$ به صورت $r = p_1^{n_1} \cdots p_k^{n_k}$ تجزیه شود ، که در آن $p_1, \ldots, p_k \in R$ اعداد اول متمایزی بوده و هر $n_i > 0$ ، آنگاه یک یکریختی R ــ مدولها مانند

$$R/(r) \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k})$$

وجود دارد . به عکس ، هر R ــ مدول دوری از مرتبهٔ r مجموع مستقیمی از k ، R ــ مدول دوری به ترتیب با مرتبه‌های $p_1^{n_1}, \ldots, p_k^{n_k}$ می‌باشد .

طرح برهان . ثابت می‌کنیم هرگاه $s, t \in R$ نسبت به هم اول باشند ، آنگاه $R/(st) \cong R/(s) \oplus R/(t)$. پس قسمت اول لم به استقرا بر تعداد اولهای متمایز در تجزیه به عوامل اول r نتیجه می‌شود . آخرین حکم لم نتیجهٔ فوری این است که ، بنابر

قضیهٔ ۴۰۶ ، $R/(c)$ یک R ــ مدول دوری از مرتبهٔ c به‌ازای هر $c \in R$ است . نگاشت $\theta : R \to R$ داده شده با $x \mapsto tx$ یک تکریختی R ــ مدولها است که ایده‌آل (s) را به روی ایده‌آل (st) می‌برد . بنابرنتیجهٔ ۸۰۱ ، θ یک همریختی R ــ مدولهای $R/(s) \to R/(st)$ القا می‌کند که با $x + (s) \mapsto tx + (st)$ داده می‌شود . به همین نحو ، یک همریختی $R/(t) \to R/(st)$ داده شده با $x + (t) \mapsto sx + (st)$ وجوددارد . بنابربرهان قضیهٔ ۱۳۰۱ ، نگاشت $\alpha : R/(s) \oplus R/(t) \to R/(st)$ داده شده با $(x + (s), y + (t)) \mapsto [tx + sy] + (st)$ یک همریختی R ــ مدولهای تعریف‌شده است . چون $(s,t) = 1_R$ ، $u,v \in R$ ای وجود دارد به‌طوری‌که $su + tv = 1_R$ (قضیهٔ III ۱۱۰۳۰) . هرگاه $c \in R$ ، آنگاه $c = suc + tvc$ ، که از آنجا $\alpha(vc + (s), uc + (t)) = c + (st)$. بنابراین ، α برووریختی است . برای نشان دادن اینکه α تکریختی است ، باید نشان دهیم که

$$\alpha(x + (s), y + (t)) = 0 \quad \Rightarrow y \in (t) \text{ و } x \in (s)$$

هرگاه $\alpha(x + (s), y + (t)) = 0$ ، آنگاه ، به‌ازای $b \in R$ ای ، $tx + sy = stb \in (st)$. از اینرو ، $utx + usy = ustb$. اما $y = 1_R y = (su + tv)y$ ، که‌ازآنجا $utx + (y - tvy) = ustb$ و $y = ustb - utx + tvy \in (t)$. استدلالی مشابه نشان می‌دهد که $x \in (s)$.

قضیهٔ ۱۲۰۶ . فرض کنیم A یک مدول با تولید متناهی روی دامنهٔ ایده‌آل اصلی R باشد .

(یک) A مجموع مستقیم زیرمدول آزاد F با رتبهٔ متناهی و تعدادی متناهی مدول تابی دوری است. جمعوندهای تابی دوری (در صورت وجود) از مرتبه‌های $r_1, \ldots, r_t$ اند ، که در آنها $r_1, \ldots, r_t$ عناصر غیر یکهٔ ناصفر (نه لزوما " متمایز ") از R اند به‌طوری‌که $r_1 \mid r_2 \mid \cdots \mid r_t$. رتبهٔ F و لیست ایده‌آلهای $(r_1), \ldots, (r_t)$ به‌طور منحصر به فرد به وسیلهٔ A معین می‌شوند .

(دو) A مجموع مستقیمی از زیرمدولهای آزاد E با رتبهٔ متناهی و تعدادی متناهی مدول تابی دوری است . جمعوندهای تابی دوری (در صورت وجود) از مرتبه‌های $p_1^{a_1}, \ldots, p_k^{a_k}$ اند ، که در آنها $p_1, \ldots, p_k$ اعداد اولی (نه لزوما " متمایز ") در R و $s_1, \ldots, s_k$ اعداد صحیح مثبتی (نه لزوما " متمایز ") می‌باشند ، رتبهٔ E و لیست ایده‌آلهای $(p_1^{a_1}), \ldots, (p_k^{a_k})$ به‌طور منحصر به فرد (جز در مورد ترتیب p_i ها) به وسیلهٔ A معین می‌شوند .

نماد $r_1|r_2|\cdots|r_t$ یعنی r_1 ، را ، r_2 ، r_3 را ، و همین‌طور تا آخر ، عاد می‌کند . عناصر $r_1, \ldots, r_t$ در قضیهٔ ۱۲.۶ را ، درست‌مثل حالت خاص گروههای آبلی ، ***عوامل پایای*** مدول A می‌نامند . به‌همین‌نحو ، $p_1^{n_1}, \ldots, p_k^{n_k}$ مقسوم ***علیه‌های مقدماتی*** A نامیده می‌شوند .

طرح برهان ۱۲.۶ . وجود تجزیهٔ مجموع مستقیم از نوع توصیف شده‌در قسمت (دو) نتیجهٔ فوری قضایای ۶.۶ ، ۷.۶ ، و ۹.۶است . لذا ، A مجموع مستقیم یک مدول آزاد و خانواده‌ای متناهی از R ــ مدولهای دوری است که هر یک مرتبه‌اش توانی از یک عنصر اول‌است . درحالت گروههای آبلی، این توانهای اول درست مقسوم علیه های مقدماتی Aمی‌باشند.در اینجا می‌توان روش محاسبهٔ عوامل پایای یک گروه آبلی از مقسوم علیه‌های مقدماتی آن (ر.ک. صفحات۱۲۴تا۱۲۵) را ***نعل به نعل*** به کار برده‌وجود تجزیهٔ مجموع مستقیم A از نوع توصیف شده در (یک) را ثابت کرد . کافی است تعدیلهای زیر صورت گیرد . نقش $Z_{p^n} \cong \mathbf{Z}/(p^n)$ ($p \in \mathbf{Z}$ اول)به وسیلهٔ یک زیرمدول تابی دوری A از مرتبهٔ p^n ($p \in R$ اول) ایفامی‌شود .طبق قضیهٔ ۴.۶ (سه) ، این مدول تابی دوری با $R/(p^n)$ یکریخت است . لم ۳.۲۰ II با لم ۱۱.۶ تعویض می‌شود .

برهان یکتایی تجزیه‌های مجموع مستقیم در (یک) و (دو) اساسا" همان برهان مطالب نظیر در گروههای آبلی است (قضیهٔ ۶.۲۰ II) . استدلال به تعدیلهای زیر نیاز دارد . پیش از همه ، تجزیه به عوامل اول در R با تقریب ضرب در یکه منحصر به فرد است (تعریف ۵.۳۰ III وقضیهٔ ۷.۳۰ III) .این مشکلی در $\mathbf{Z}$ پیش نمی‌آورد ، زیرا تنها یکه‌ها ± 1 بودوو عناصر اول مثبت‌تعریف شده‌اند . اما ، در دامنهٔ ایده‌آل اصلی دلخواه R ، عنصر $a \in R$ ممکن است دارای مرتبهٔ p و مرتبهٔ q باشد و p,q عناصر اول متمایزی باشند . با اینحال ، چون $(p) = \mathcal{O}_a = (q)$ ،طبق قضیهٔ ۲.۳۰ III ، q, p با هم شریکند ؛ یعنی ، $q = pu$ ، که در آن $u \in R$ یکه است . از اینرو ، احکام یکتایی در (یک) و (دو) با ایده‌آلها سر و کار دارند تا عناصر . توجه کنید که $a \neq 0$ ایجاب می‌کند که $\mathcal{O}_a \neq R$ و یک مدول دوری Ra آزاد است اگر و فقط‌اگر $\mathcal{O}_a = (0)$. لذا ، عناصر r_i در (یک) غیریکه‌های ناصفرند . تعدیلهای دیگر : مثل فوق ، هر جمعوند دوری متناهی $Z_n \cong \mathbf{Z}/(n)$ ، که $n > 1$ ، رابامدول‌تابی‌دوری $R/(r)$ ($r \in R$ یک غیریکهٔ ناصفر است) عوض کنید . زیرگروه تولید شده به وسیلهٔ جمعوندهای دوری نامتناهی $\mathbf{Z}$ را با یک

R ــ مدول‌بارتبهٔ متناهی عوض کنید. از لمهای ۱۰۰۶ و ۱۱۰۶ به جای لمهای II ۳۰۲۰ و II ۵۰۲۰ استفاده‌کنید. به‌جای‌استدلال‌شمارشی در ص۱۲۲ (که نشان می‌دهد $r = d$)، از این استفاده کنید که $A[p]$ یک فضای برداری روی $R/(p)$ است. از اینرو، تعداد جمعوندهای $R/(p)$ دقیقا" $\dim_{R/(p)} A[p]$ است، که طبق قضیهٔ ۷۰۲، پایا می‌باشد.

نتیجهٔ ۱۳۰۶. *دو مدول با تولید متناهی* A و B *روی یک دامنهٔ ایده‌آل اصلی یکریخت‌اند اگر و فقط اگر* A/A_t و B/B_t *رتبه‌های یکسان داشته و عوامل پایای [یا مقسوم‌علیه‌های مقدماتی]* A و B *یکی باشند.*

برهان. تمرین.

تمرینات

تذکر. R یک دامنهٔ ایده‌آل اصلی است و تمام مدولها یکانی‌اند، مگر آنکه خلافش تصریح شود.

۱. هرگاه R حلقه‌ای تعویضپذیر و یکدار باشد به‌طوری‌که هر زیرمدول یک R ــ مدول آزاد آزاد باشد، آنگاه R یک دامنهٔ ایده‌آل اصلی است. [**راهنمایی.** هر ایده‌آل I از R یک R ــ مدول آزاد است. هرگاه $u,v \in I$ $(u \neq 0, v \neq 0)$، آنگاه $uv + (-v)u = 0$، که ایجاب می‌کند که I دارای پایه‌ای با یک عنصر است؛ یعنی، I اصلی است.]

۲. هر مدول آزاد روی یک دامنهٔ صحیح دلخواه یکدار فارغ از تاب است. عکس مطلب درست نیست (تمرین II ۱۰۰۱۰).

۳. فرض کنید A یک R ــ مدول دوری از مرتبهٔ $r \in R$ باشد.
(آ) هرگاه $s \in R$ نسبت به r اول باشد، آنگاه $sA = A$ و $A[s] = 0$.
(ب) هرگاه s، r را عاد کند، مثلا" $sk = r$، آنگاه $sA \cong R/(k)$ و $A[s] \cong R/(s)$.

۴. هرگاه A یک R ــ مدول دوری از مرتبهٔ r باشد، آنگاه (یک) هر زیرمدول A دوری است با مرتبه‌ای که r را عاد می‌کند؛ (دو) به‌ازای هر ایده‌آل (s) شامل (r)، A دقیقا" یک زیرمدول دارد، که دوری از مرتبهٔ s است.

۵. هرگاه A مدول تابی با تولید متناهی باشد، آنگاه $\{r \in R \mid rA = 0\}$ ایده‌آلی ناصفر

در R است، مثلاً " $(r_1) \cdot r_1$ **صفرساز مینیمال** A نام دارد. فرض کنید A یک گروه آبلی متناهی با صفرساز مینیمال $m \in \mathbf{Z}$ باشد. نشان دهید که زیرگروه دوری A از مرتبه‌ای که حقیقتاً " m را عاد می‌کند لزوماً " یک جمعوند مستقیم A نیست.

۶. هرگاه A و B مدولهایی دوری روی R و به ترتیب از مرتبه‌های r و s باشند، و r نسبت به s اول **نباشد**، آنگاه عوامل پایای $A \oplus B$ بزرگترین مقسوم‌علیه مشترک r,s و کوچکترین مضرب مشترک r,s می‌باشند.

۷. فرض کنید A و $a \in A$ در مفروضات لم ۸.۶ صدق کنند.

(آ) هر Rـ زیر مدول A یک $R/(p^n)$ ــ مدول است که $(r + (p^n))a = ra$. به عکس، هر $R/(p^n)$ ــ زیرمدول A یک R ــ زیرمدول به‌وسیلهٔ برگشت در امتداد $R \to R/(p^n)$ است.

(ب) زیرمدول Ra با $R/(p^n)$ یکریخت است.

(پ) تنها ایده‌آلهای حقیقی حلقهٔ $R/(p^n)$ ایده‌آلهای تولید شده به وسیلهٔ $(i = 1,2,\ldots,n-1)\ p^i + (p^n)$ اند.

(ت) $R/(p^n)$ (و درنتیجه، Ra) یک انژکتیو $R/(p^n)$ ــ مدول است.

[**راهنمایی.** از (پ) و لم ۸.۳ استفاده کنید.]

(ث) یک R ــ زیرمدول از A مانند C هست به‌طوری‌که $A = Ra \oplus C$.

[**راهنمایی.** حکم ۱۳.۳.]

۷ جبرها

جبرها را معرفی کرده وخواص اساسی آنها را عرضه می‌کنیم. در این بحث، حاصلضربهای تانسوری به‌طرز وسیعی به‌کار می‌روند. جبرها در فصل نه بیشتر مورد مطالعه قرار خواهند گرفت.

تعریف ۱.۷. فرض کنیم K یک حلقهٔ تعویضپذیر یکدار باشد. **K ــ جبر** (یا **جبر روی** K) A حلقه‌ای است که

(یک) $(A,+)$ یک K ــ مدول (چپ) یکانی است؛

(دو) به‌ازای هر $k \in K$ و $a,b \in A$، $k(ab) = (ka)b = a(kb)$.

K ــ جبر A که، به عنوان حلقه، یک حلقهٔ بخشی است، یک **جبر بخشی** نام دارد.

نظریهٔ کلاسیک جبرهابه جبرهای روی میدان K می‌پردازد. یک چنین جبر فضایی برداری روی K است؛ و درنتیجه، نتایج مختلف جبر خطی قابل اعمالند. یک جبر روی میدان K که به‌عنوان فضایی برداری روی K با بعد متناهی باشد یک **جبر با بعد متناهی** روی K نام دارد.

مثال. هر حلقهٔ R یک گروه آبلی جمعی، و درنتیجه یک $\mathbf{Z}$ ــ مدول، است. به آسانی معلوم می‌شود که R عملاً" یک $\mathbf{Z}$ ــ جبر است.

چند مثال. هرگاه K حلقه‌ای تعویضپذیر و یکدار باشد، آنگاه حلقهٔ چندجمله‌ای $K[x_1, \ldots, x_n]$ و حلقهٔ سریهای توانی $K[[x]]$ ، K ــ جبرند با ساختارهای K ــ مدولی که به طریق معمول بدانها داده می‌شوند.

مثال. هرگاه V فضایی برداری روی میدان F باشد، آنگاه حلقهٔ درونریختی $\mathrm{Hom}_F(V,V)$ (تمرین ۷.۱) یک F ــ جبر است. ساختار F ــ مدول $\mathrm{Hom}_F(V,V)$ در تبصرهٔ بعد از قضیهٔ ۸.۴ مطرح شد.

چند مثال. فرض کنیم A حلقه‌ای یکدار بوده و K زیرحلقه‌ای به مرکز A باشد به‌طوری‌که $1_A \in K$. در این صورت، A یک K ــ جبر است، با ساختار K ــ مدولی که با ضرب در A داده می‌شود. بخصوص، هر حلقهٔ تعویضپذیر یکدار K یک K ــ جبر است.

مثال. میدان اعداد مختلط $\mathbf{C}$ و حلقهٔ بخشی چهارتاهای حقیقی (ص ۱۸۲) هر دو جبرهای بخشی روی میدان $\mathbf{R}$ از اعداد حقیقی می‌باشند.

مثال. فرض کنیم G گروهی ضربی و K حلقه‌ای تعویضپذیر و یکدار باشد. در این صورت، حلقهٔ گروهی $K(G)$ (ص ۱۸۱) عملاً" یک K ــ جبر با ساختار K ــ مدول داده شده با

$$k(\sum r_i g_i) = \sum (kr_i) g_i \qquad (k, r_i \in K;\ g_i \in G)$$

است. $K(G)$ **جبر گروهی** G روی K نام دارد.

مثال. هرگاه K یک حلقهٔ تعویضپذیر و یکدار باشد، آنگاه حلقهٔ $\mathrm{Mat}_n K$ مرکب از تمام ماتریسهای $n \times n$ روی K یک K ــ جبر است، که عمل K ــ مدول K به طریق معمول داده‌شده‌است. به‌طورکلی، هرگاه A یک K ــ جبر باشد، آنگاه $\mathrm{Mat}_n A$ نیز چنین است.

تبصره. چون K تعویضپذیر است، هر K ــ مدول چپ (و درنتیجه، هر K ــ جبر) A نیز یک K ــ مدول راست است، که در آن به‌ازای هر $a \in A, k \in K$، $ka = ak$. این امر تلویحاً در قضایای ۲۰۷ و ۴۰۷ در زیر، که در آنها از حاصلضربهای تانسوری استفاده می‌شود، فرض شده است.

انگیزهٔ قضیهٔ بعد، که وسایل دیگر تعریف K ــ جبرها را فراهم می‌کند، این است که به‌ازای هر حلقهٔ R، نگاشت منحصربه‌فرد $R \otimes_{\mathbf{Z}} R \to R$ تعریف شده بر یک مولد مانند $r \otimes s$ با $r \otimes s \mapsto rs$ یک همریختی از گروههای آبلی جمعی است. چون حلقه‌ها چیزی جز $\mathbf{Z}$ ــ جبرها نیستند، این امر حالت خاصی از قضیهٔ زیر است.

قضیهٔ ۲۰۷. *فرض کنیم K حلقه‌ای تعویضپذیر و یکدار بوده و A یک K ــ مدول چپ یکانی باشد. دراین‌صورت، A یک K ــ جبر است اگر و فقط اگر یک همریختی K ــ مدولها مانند $\pi : A \otimes_K A \to A$ موجود باشد به‌طوری‌که نمودار*

$$\begin{array}{ccc} A \otimes_K A \otimes_K A & \xrightarrow{\pi \otimes 1_A} & A \otimes_K A \\ \downarrow{\scriptstyle 1_A \otimes \pi} & & \downarrow{\scriptstyle \pi} \\ A \otimes_K A & \xrightarrow{\pi} & A \end{array}$$

تعویضپذیر باشد. در این حالت، K ــ جبر A یکدار است اگر و فقط اگر یک همریختی K ــ مدولها مانند $I : K \to A$ وجود داشته باشد به‌طوری‌که نمودار

$$\begin{array}{ccccc} K \otimes_K A & \xrightarrow{\xi} & A & \xleftarrow{\theta} & A \otimes_K K \\ \downarrow{\scriptstyle I \otimes 1_A} & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle 1_A \otimes I} \\ A \otimes_K A & \xrightarrow{\pi} & A & \xleftarrow{\pi} & A \otimes_K A \end{array}$$

تعویضپذیر باشد، که در آن ξ, θ یکریختیهای قضیهٔ ۷۰۵ است.

طرح برهان. هرگاه A یک K ــ جبر باشد، آنگاه نگاشت $A \times A \to A$ داده شده با $(a,b) \mapsto ab$، K ــ دوخطی است؛ پس، بنابر قضیهٔ ۶۰۵، یک همریختی K ــ مدولها مانند

$$\pi : A \otimes_K A \to A$$

وجود دارد؛ تحقیق کنید که π خواص مطلوب را داراست. هرگاه A دارای واحد 1_A باشد، آنگاه به آسانی معلوم می‌شود که نگاشت $I : K \to A$ داده شده با $k \mapsto k1_A$ یک همریختی K ــ مدولها با خواص مطلوب است. به عکس، اگر A و نگاشت $\pi : A \otimes_K A \to A$ داده شده باشند، تعریف کنید $ab = \pi(a \otimes b)$ و تحقیق کنید که A یک K ــ جبر است. اگر $I : K \to A$ نیز داده شده باشد، آنگاه $I(1_K)$ یک همانی برای A است.

همریختی π قضیهٔ ۲۰۷ **نگاشت حاصلضربی** K ــ جبر A نام دارد. همریختی I **نگاشت یکه** نامیده می‌شود.

تعریف ۳۰۷. فرض کنیم K یک حلقهٔ تعویضپذیر و یکدار بوده و A, B ، K ــ جبر باشند.

(یک) هر **زیرجبر** A یک زیرحلقهٔ A است که یک K ــ زیرمدول A نیز هست.

(دو) هر **ایده‌آل جبر** (چپ، راست، دوطرفه) A یک ایده‌آل (چپ، راست، دوطرفه) حلقهٔ A است که یک K ــ زیرمدول A نیز هست.

(سه) هر **همریختی [یکریختی]** K ــ جبرهای $f : A \to B$ یک‌همریختی [یکریختی] است که یک همریختی [یکریختی] K ــ مدولها نیز هست.

چند تبصره. اگر A یک K ــ جبر باشد، یک ایده‌آل حلقهٔ A لزوما " یک ایده‌آل جبر A نیست (تمرین ۴). اما، هرگاه A یکدار باشد، آنگاه، به‌ازای هر $k \in K$ و $a \in A$،

$$ka = (ka)1_A = a(k1_A) \quad \text{و} \quad ka = k(1_A a) = (k1_A)a$$

که در آنها $k1_A \in A$. درنتیجه، برای یک ایده‌آل چپ [راست] J در حلقهٔ A،

$$kJ = (k1_A)J \subset J \quad [\, kJ = J(k1_A) \subset J \,].$$

بنابراین، اگر A یکدارباشد، هرایده‌آل (چپ، راست، دوطرفه) یک ایده‌آل جبر (چپ، راست، دوطرفه) می‌باشد.

حال جبرخارج‌قسمتی K ــ جبر A بر ایده‌آل‌جبر I به طرزروشنی تعریف می‌شود؛ به همین ترتیب، حاصل‌ضرب مستقیم و مجموع مستقیم خانواده‌ای از K ــ جبرها را خواهیم داشت.

حاصل‌ضربهای‌تانسوری‌راه دیگری برای تولید جبرهای جدید به دست می‌دهند. ابتدا ملاحظه می‌کنیم که هرگاه A و B، Kــ مدول باشند، آنگاه یک یکریختی K ــ مدولها مانند $\alpha : A \otimes_K B \to B \otimes_K A$ وجود دارد به‌طوری‌که $\alpha(a \otimes b) = b \otimes a$ $(a \in A, b \in B)$؛ ر.ک. تمرین ۲.

قضیهٔ ۴۰۷. *فرض کنیم A و B جبرهایی [یکدار] روی حلقهٔ تعویضپذیر و یکدار K باشند. همچنین، π ترکیب*

$$(A \otimes_K B) \otimes_K (A \otimes_K B) \xrightarrow{1_A \otimes \alpha \otimes 1_B} (A \otimes_K A) \otimes_K (B \otimes_K B) \xrightarrow{\pi_A \otimes \pi_B} A \otimes_K B$$

باشد، که در آن π_A, π_B به‌ترتیب نگاشتهای حاصل‌ضربی A و B باشند. در این صورت، $A \otimes_K B$ یک K ــ جبر [یکدار] با نگاشت حاصل‌ضربی π است.

برهان. تمرین: توجه‌کنیدکه برای مولدهای $a \otimes b$ و $a_1 \otimes b_1$ از $A \otimes_K B$، حاصل‌ضرب مساوی

$$(a \otimes b)(a_1 \otimes b_1) = \pi(a \otimes b \otimes a_1 \otimes b_1) = aa_1 \otimes bb_1$$

تعریف شده است. لذا، هرگاه A و B به ترتیب دارای واحدهای $1_A, 1_B$ باشند، آنگاه $1_A \otimes 1_B$ واحد $A \otimes_K B$ است.

قضیهٔ ۴۰۷ *حاصل‌ضرب تانسوری K ــ جبرهای A و B است.* $A \otimes_K B$ K ــ جبر است. حاصل‌ضربهای تانسوری جبرها در بررسی ساختار جبرهای بخشی روی میدان K مفیدند (بخش IX: ۶).

تمرینات

تذکر. K همواره یک حلقهٔ تعویضپذیر و یکدار است.

۱. فرض کنید $\mathfrak{C}$ رسته‌ای باشد که اشیاء آن همهٔ K ــ جبرهای تعویضپذیر یکدار و ریختهایش همهٔ همریختیهای K ــ جبرهای $f : A \to B$ اند به‌طوری که $f(1_A) = 1_B$.

در این صورت، هر دو K ــ جبر A, B از $\mathcal{C}$ دارای هم حاصلضرب می باشند. [**راهنمایی.** $A \to A \otimes_K B \leftarrow B$ را درنظر بگیرید، که در آن $a \mapsto a \otimes 1_B$ و $b \mapsto 1_A \otimes b$.]

۲. هرگاه A و B ، K ــ مدولهایی [K ــ جبرهایی] یکانی باشند، آنگاه یک یکریختی K ــ مدولها [K ــ جبرها] مانند $\alpha : A \otimes_K B \to B \otimes_K A$ وجود دارد بهطوری‌که بهازای هر $a \in A, b \in B$ ، $\alpha(a \otimes b) = b \otimes a$.

۳. فرض کنید A حلقه‌ای یکدار باشد. در این‌صورت، A یک K ــ جبر یکدار است اگر و فقط اگر یک همریختی حلقه‌ها از K به توی مرکز A وجود داشته باشد به طوری‌که $1_K \mapsto 1_A$.

۴. فرض کنید A یک فضای برداری یک‌بعدی روی میدان گویای $\mathbf{Q}$ باشد. هرگاه بهازای هر $a, b \in A$ تعریف کنیم $ab = 0$ ، آنگاه A یک $\mathbf{Q}$ ــ جبر است. هر زیرگروه جمعی حقیقی A یک ایده‌آل حلقهٔ A است، ولی یک ایده‌آل جبر نیست.

۵. فرض کنید $\mathcal{C}$ رستهٔ تمرین ۱ باشد. هرگاه X مجموعهٔ $\{x_1, \ldots, x_n\}$ باشد، آنگاه جبر چندجمله‌ایهای $K[x_1, \ldots, x_n]$ یک شیٔ آزادبر مجموعهٔ X در رستهٔ $\mathcal{C}$ است. [**راهنمایی.** بهازای جبر A در $\mathcal{C}$ و نگاشت $g : \{x_1, \ldots, x_n\} \to A$ ، قضیهٔ III ۵۰۵۰ را در مورد نگاشت یکتای $I : K \to A$ و عناصر $g(x_1), \ldots, g(x_n) \in A$ به کار برید.]

۵

میدانها و نظریهٔ گالوا[1]

اولین مطلب اساسی این فصل نظریهٔ ساختاری میدانهاست. ما میدان F را برحسب یک زیرمیدان مشخص K مطالعه می‌کنیم (گوییم F یک توسیع میدان K است). نکات اصلی درباب توسیعهای میدان، بویژه، تمایز بین توسیعهای جبری و متعالی، در بخش ۱ داده می‌شوند. در اکثر جاهای این فصل فقط با توسیعهای جبری سر و کار داریم. توسیعهای دلخواه میدان در فصل شش مطرح می‌شوند. ساختار بعضی از میدانها و توسیعهای میدان کاملاً تحلیل می‌شوند: توسیعهای ساده (بخش ۱)؛ میدانهای تجزیه‌گر (توسیعهای نرمال) و بستهای جبری (بخش ۳)؛ میدانهای متناهی (بخش ۵)؛ و توسیعهای جبری جدایی‌پذیر (بخشهای ۳ و ۶).

نظریهٔ گالوا در توسیعهای میدان (مطلب اصلی دیگر این فصل) ریشه‌ای تاریخی درمسئلهٔ کلاسیکی از نظریهٔ معادلات دارد، که به تفصیل در بخشهای ۴ و ۹ مطرح شده است. نتایج مختلف نظریهٔ گالوا کاربردهای مهمی، بویژه در بررسی اعداد جبری (ر.ک. ای. آرتین[2] [۴۸]) و هندسهٔ جبری (ر.ک. اس. لانگ[3] [۵۴]) دارد.

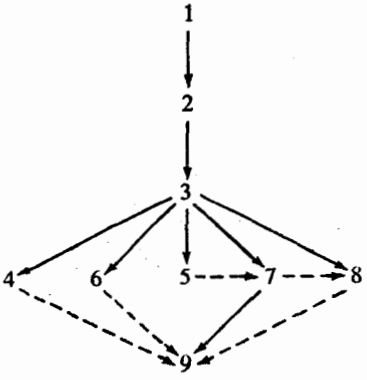
ایدهٔ کلیدی نظریهٔ گالوا ارتباط توسیع میدان $K \subset F$ به گروه تمام خودریختیهای F است که K را عنصروارثابت نگه می‌دارند (گروه توسیع گالوا). یک توسیع میدان گالوا را می‌توان برحسب گروه گالوای آن (بخش ۲) یا برحسب ساختار داخلی آن (بخش ۳)

---

1. Galois
2. E. Artin
3. S. Lang

تعریف کـرد . قضیهٔ اسـاسی نظـریهٔ گالوا (بخش ۲) می‌گوید که تناظر یک به یکی بین میدانهای‌میانی یک توسیع میدان گالوا (با بعد متناهی) و زیرگروههای گروه توسیع گالوا وجوددارد .این‌قضیه به‌ما امکان‌ترجمهٔ خواص و مسائل مربوط به میدانها ، چندجمله‌ایها ، و تـوسیعهای میـدان را به زبان نظریهٔ گروهها می‌دهد . بسیار اتفاق می‌افتد که مسئلهٔ نظیر در گروهها جواب دارد ، و از آنجا می‌توان مسئلهٔ اصلی را در نظریهٔ میدانها حل کرد . مثلا" ، مسئلهٔ کلاسیک نظریهٔ معادلات که در بندپیش ذکر شد چنین است . ما آن توسیعهای میدان گالوا را توصیف می‌کنیم که گروههای گالوای آنها دوری متناهی (بخش ۷) یا حلپذیر (بخش ۹ باشند.

ارتباط تقریبی بخشهای این فصل به صورت زیر است :



سهم شکسته مبین آن است که از نتایج بخش A گهگاه در بخش B استفاده می‌شود ، ولی B اساسا" مستقـل از بخش A است .***برای توصیفی از یک درس اساسی کوتاه در میدانها و نظریهٔ گالوا، ر.ک. صفحهٔ ز.***

۱ توسیعهای میدان

ابتدا مطالب اصلی لازم برای مطالعهٔ توسیعهای میدان را عرضه کرده ، سپس توسیعهای ساده‌را مطرح می‌کنیم . بالاخره ، چند خاصیت اساسی توسیعهای جبری را ثابت می‌کنیم . در ضمیمه ، کـه در آینده بـه کار نمی‌آید ، چنـد مسئلهٔ هندسی مشهور قدیمی ، ازقبیل تثلیث زاویه به وسیلهٔ خط‌کش و پرگار ، سامان خواهند یافت .

تعریف ۱۰۱ . گوییم میدان F یک **توسیع میدان** K (یا فقط توسیع K) است مشروط بر اینکه K زیرمیدانی از F باشد .

هرگاه F یک توسیع میدان K باشد ، آنگاه به‌آسانی معلوم می‌شود که $1_K = 1_F$. به علاوه ، F یک فضای‌برداری‌روی K است (تعریف IV ۱۰۱۰) .درسراسر این فصل ، بعد K ــ فضای برداری F ، به جـای $\dim_K F$ مثل قبل ، با $[F:K]$ نموده می‌شود . گوییم F یک **تـوسیع بـا بعد متناهی** یا **توسیع با بعد نامتناهی** از K است بسته به اینکه $[F:K]$ متناهی یا نامتناهی باشد .

قضیهٔ ۲۰۱ . *فرض‌کنیم F یک تـوسیع میدان E و E یک توسیع میدان K باشد . در این صورت ،* $[F:K] = [F:E][E:K]$. **به عـلاوه ،** $[F:K]$ ***متناهی است اگر و فقط اگر*** $[F:E]$ **و** $[E:K]$ **متناهی باشند .**

برهان . این بیان دیگری است از قضیهٔ IV ۱۶۰۲۰ .

در وضعیت $K \subset E \subset F$ قضیـهٔ ۲۰۱ ، گوییم E یک **میدان میانی** K و F است .

هرگاه F میدان‌بوده‌و $X \subset F$ ، آنگاه **زیرمیدان [زیرحلقهٔ] تولید شده به وسیلهٔ X** اشتراک تمام زیرمیدانها [زیرحلقه‌ها]ی F است که شامل X اند . هرگاه F یک توسیع میـدان K بـوده و $X \subset F$ ، آنگاه زیرمیدان [زیرحلقهٔ] تولید شده به وسیلهٔ $K \cup X$ **زیرمیدان [زیرحلقهٔ] تولید شده بـه وسیلهٔ X** روی **K** نام دارد و با نماد $K(X)$ [$K[X]$] نموده می‌شود . توجه کنید که $K[X]$ لزوما " یک دامنهٔ صحیح است .

هرگـاه $X = \{u_1, \ldots, u_n\}$ ، آنـگاه زیـرمیـدان $K(X)$ [زیـرحلقهٔ $K[X]$] با F $K(u_1, \ldots, u_n)$ [$K[u_1, \ldots, u_n]$] نموده‌می‌شود . گوییم میدان $K(u_1, \ldots, u_n)$ یک **توسیع با تولید متناهی** است (ولی‌لازم‌نیست‌روی K با بعد متناهی باشد ؛ ر.ک. تمرین ۲) . هرگاه $X = \{u\}$ ، گوییم $K(u)$ یک **توسیع سـادهٔ** K است . تحقیقی عادی نشان می‌دهد کـه هیچیـک از $K(u_1, \ldots, u_n)$ یـا $K[u_1, \ldots, u_n]$ بـه مـرتبـهٔ u_i بستگـی نـدارند و $K(u_1, \ldots, u_{n-1})(u_n) = K(u_1, \ldots, u_n)$ و $K[u_1, \ldots, u_{n-1}][u_n] = K[u_1, \ldots, u_n]$ (تمرین ۴) . از این نکات بارها در آینده به‌طور تلویحی استفاده خواهیم کرد .

نمادگذاری. هرگاه F یک میدان بوده، $u,v \in F$، و $v \neq 0$، آنگاه گاهی $uv^{-1} \in F$ را با u/v نشان می‌دهیم.

قضیهٔ ۳۰۱. هرگاه F یک‌توسیع میدانی میدانی مانند K بوده، $u, u_i \in F$، و $X \subset F$، آنگاه

(یک) زیرحلقهٔ $K[u]$ از تمام عناصر به شکل $f(u)$ تشکیل شده است، که در آن f یک چندجمله‌ای با ضرایب در K است (یعنی، $f \in K[x]$)؛

(دو) زیرحلقهٔ $K[u_1, \ldots, u_m]$ از تمام عناصر به شکل $g(u_1, u_2, \ldots, u_m)$ تشکیل شده است، که در آن g یک چندجمله‌ای از m مجهول با ضرایب در K است (یعنی، $g \in K[x_1, \ldots, x_m]$)؛

(سه) زیرحلقهٔ $K[X]$ از تمام عناصر به شکل $h(u_1, \ldots, u_n)$ تشکیل شده است، که در آن هر $u_i \in X$، n عددصحیح مثبتی است، و h یک چندجمله‌ای با n مجهول و ضرایب در K می‌باشد (یعنی، $n \in \mathbf{N}^*, h \in K[x_1, \ldots, x_n]$)؛

(چهار) زیرمیدان $K(u)$ از تمام عناصر به شکل $f(u)/g(u) = f(u)g(u)^{-1}$ تشکیل شده است، که در آن $f,g \in K[x]$ و $g(u) \neq 0$؛

(پنج) زیرمیدان $K(u_1, \ldots, u_m)$ از تمام عناصر به شکل

$$h(u_1, \ldots, u_n)/k(u_1, \ldots, u_n) = h(u_1, \ldots, u_n)k(u_1, \ldots, u_n)^{-1}$$

تشکیل شده است، که در آن $h,k \in K[x_1, \ldots, x_m]$ و $k(u_1, \ldots, u_m) \neq 0$؛

(شش) زیرمیدان $K(X)$ از تمام عناصر به شکل

$$f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) = f(u_1, \ldots, u_n)g(u_1, \ldots, u_n)^{-1}$$

تشکیل شده است، که در آن $n \in \mathbf{N}^*$، $f,g \in K[x_1, \ldots, x_n]$، $u_1, \ldots, u_n \in X$، و $g(u_1, \ldots, u_n) \neq 0$.

(هفت) به‌ازای هر $v \in K(X)$ ($K[X]$)، یک زیرمجموعهٔ متناهی از X مانند X' هست به‌طوری که $v \in K(X')$ ($K[X']$).

طرح برهان. (شش) هر میدان شامل K و X باید شامل

$$E = \{ f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) \mid n \in \mathbf{N}^*;\ f,g \in K[x_1, \ldots, x_n];\ u_i \in X;\ g(u_1, \ldots, u_n) \neq 0 \}$$

باشد، که از آنجا $K(X) \supset E$. به‌عکس، هرگاه $f,g \in K[x_1, \ldots, x_m]$ و $f_1,g_1 \in K[x_1, \ldots, x_n]$، آنگاه $h,k \in K[x_1, \ldots, x_{m+n}]$ را با

$$h(x_1, \ldots, x_{m+n}) = f(x_1, \ldots, x_m)g_1(x_{m+1}, \ldots, x_{m+n}) - g(x_1, \ldots, x_m)f_1(x_{m+1}, \ldots, x_{m+n});$$
$$k(x_1, \ldots, x_{m+n}) = g(x_1, \ldots, x_m)g_1(x_{m+1}, \ldots, x_{m+n})$$

تعریف می‌کنیم. در این صورت، به‌ازای هر $u_1, \ldots, u_m, v_1, \ldots, v_n \in X$ که $g(u_1, \ldots, u_m) \neq 0, g_1(v_1, \ldots, v_n) \neq 0$

$$\frac{f(u_1, \ldots, u_m)}{g(u_1, \ldots, u_m)} - \frac{f_1(v_1, \ldots, v_n)}{g_1(v_1, \ldots, v_n)} = \frac{h(u_1, \ldots, u_m, v_1, \ldots, v_n)}{k(u_1, \ldots, u_m, v_1, \ldots, v_n)} \in E.$$

بنابراین، E یک گروه تحت جمع است (قضیهٔ I ۵.۲۰). به همین نحو، عناصر ناصفر E تحت ضرب گروه تشکیل می‌دهند، که از آنجا E یک میدان می‌باشد. چون $X \subset E$ و $K \subset E$، داریم $K(X) \subset E$. بنابراین، $K(X) = E$. (هفت) هرگاه $u \in K(X)$، آنگاه بنابر (شش)، $u = f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) \in K(X')$، که در آن $X' = \{u_1, \ldots, u_n\} \subset X$.

اگر L و M زیرمیدانهایی از میدان F باشند، **ترکیب** L و M در F، که با LM نموده می‌شود، زیرمیدان تولید شده به وسیلهٔ مجموعهٔ $L \cup M$ است. یک نتیجهٔ مهم از این تعریف این است که $LM = L(M) = M(L)$. به‌آسانی معلوم می‌شود که هرگاه K زیرمیدانی از $L \cap M$ باشد به‌طوری‌که $M = K(S)$، که در آن $S \subset M$، آنگاه $LM = L(S)$ (تمرین ۵). روابط بین بعدهای $[L : K], [M : K], [LM : K]$ و غیره در تمرینات ۲۰ تا ۲۱ درنظرگرفته شده‌اند. ترکیب هر تعداد متناهی زیرمیدان $E_1, E_2, \ldots, E_n$ مساوی زیرمیدان تولید شده به وسیلهٔ $E_1 \cup E_2 \cup \cdots \cup E_n$ تعریف شده و با $E_1E_2 \cdots E_n$ نموده می‌شود (ر.ک. تمرین ۵).

قدم بعدی در مطالعهٔ توسیعهای میدان تشخیص دو وضعیت اساسا" متفاوت است.

تعریف ۴.۱. فرض کنیم F یک توسیع میدان K باشد. گوییم عنصر u از F روی K **جبری** است مشروط بر اینکه u ریشهٔ یک چندجمله‌ای ناصفر مانند $f \in K[x]$ باشد. اگر u ریشهٔ هیچ $f \in K[x]$ ناصفر نباشد، گوییم u روی K **متعالی** است. F یک **توسیع جبری** K نام دارد اگر هر عنصر F روی K جبری باشد. F یک **توسیع متعالی** نامیده می‌شود اگر دست‌کم یک عنصر F روی K متعالی باشد.

چند تبصره. هرگاه $u \in K$، آنگاه u ریشه‌ای از $x - u \in K[x]$ است؛ و لذا، روی K

جبری می‌باشد. هرگاه $u \in F$ روی زیر میدانی از K مانند K' جبری باشد، آنگاه u روی K جبری است، زیرا $K'[x] \subset K[x]$. هرگاه $u \in F$ ریشه‌ای از $f \in K[x]$ با ضریب پیشرو $c \neq 0$ باشد، آنگاه u ریشه‌ای از $c^{-1}f$ نیز هست، که یک چندجمله‌ای تکین در $K[x]$ می‌باشد. توسیع متعالی ممکن است (علاوه بر خود عناصر K) شامل عناصری باشد که روی K جبری‌اند.

چند مثال. فرض کنیم $\mathbf{Q}$، $\mathbf{R}$، و $\mathbf{C}$ به‌ترتیب میدانهای اعداد گویا، حقیقی، و مختلط باشند. در این صورت، $i \in \mathbf{C}$ روی $\mathbf{Q}$، و درنتیجه روی $\mathbf{R}$، جبری است؛ درواقع، $\mathbf{C} = \mathbf{R}(i)$. نکته‌ای نه‌چندان بدیهی متعالی بودن $\pi, e \in \mathbf{R}$ روی $\mathbf{Q}$ است؛ مثلاً"، ر.ک. آی. هراشتاین[1] [۴].

مثال. هرگاه K یک میدان باشد، آنگاه حلقهٔ چندجمله‌ای $K[x_1, \ldots, x_n]$ یک دامنه صحیح است (قضیهٔ ۳۰۵۰ III). میدان خارج‌قسمتی $K(x_1, \ldots, x_n)$ با $K[x_1, \ldots, x_n]$ نموده می‌شود. این میدان از تمام کسرهای f/g تشکیل شده است، که $f, g \in K[x_1, \ldots, x_n]$ و $g \neq 0$، و جمع و ضرب آن معمولی‌اند (ر.ک. قضیهٔ ۳۰۴۰ III). $K(x_1, \ldots, x_n)$ **میدان توابع گویا** از $x_1, \ldots, x_n$ روی K نام دارد. در توسیع میدان

$$K \subset K(x_1, \ldots, x_n)$$

به‌آسانی دیده می‌شود که هر x_i روی K متعالی است. درواقع، هر عنصر $K(x_1, \ldots, x_n)$ که در خود K نباشد روی K متعالی است (تمرین ۶).

دردو قضیهٔ زیر، تمام توسیعهای میدان ساده را با تقریب یکریختی مشخص خواهیم کرد.

قضیهٔ ۵۰۱. *هرگاه F یک توسیع میدان K بوده و $u \in F$ روی K متعالی باشد، آنگاه یک یکریختی از میدانها مانند $K(u) \cong K(x)$ وجود دارد که بر K همانی است.*

طرح برهان. چون u متعالی است، به‌ازای هر $f, g \in K[x]$ ناصفر، $f(u) \neq 0$, $g(u) \neq 0$.

---

1. I. Herstein

درنتیجه، نگاشت $\varphi : K(x) \to F$ داده شده با $f/g \mapsto f(u)/g(u) = f(u)g(u)^{-1}$ یک تکریختی تعریف‌شده ازمیدانهاست که بر K همانی است. اما، طبق قضیهٔ ۳۰۱، $\operatorname{Im} \varphi = K(u)$ که از آنجا $K(x) \cong K(u)$.

قضیهٔ ۶۰۱. *هرگاه F یک توسیع میدان K بوده و $u \in F$ روی K جبری باشد، آنگاه*

(یک) $K(u) = K[u]$؛

(دو) $K(u) \cong K[x]/(f)$، *که در آن $f \in K[x]$ یک چندجمله‌ای تکین تحویل‌ناپذیر از درجهٔ $n \geq 1$ است که با شرایط $f(u) = 0$ و $(g \in K[x])\ g(u) = 0$ اگر و فقط اگر f، g را عاد کند، به‌طور منحصر به فرد معین می‌شود*؛

(سه) $[K(u) : K] = n$؛

(چهار) *پایه‌ای از فضای برداری $K(u)$ روی K است*؛ $\{1_K, u, u^2, \ldots, u^{n-1}\}$

(پنج) *هر عنصر $K(u)$ را می‌توان به‌طور منحصر به فرد به شکل $a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$ $(a_i \in K)$ نوشت.*

برهان. (یک) و (دو). نگاشت $\varphi : K[x] \to K[u]$ داده شده با $g \mapsto g(u)$، طبق قضایای III ۵۰۵۰ و ۳۰۱، یک بروریختی ناصفر حلقه‌هاست. چون $K[x]$ یک دامنهٔ ایده‌آل اصلی است (نتیجهٔ III ۴۰۶۰)، به‌ازای $f \in K[x]$ ی که $f(u) = 0$، $\operatorname{Ker} \varphi = (f)$. چون u جبری است، $\operatorname{Ker} \varphi \neq 0$، و چون $\varphi \neq 0$، $\operatorname{Ker} \varphi \neq K[x]$. از اینرو، $f \neq 0$ و $\deg f \geq 1$. به علاوه، اگر c ضریب پیشرو f باشد، آنگاه c یک یکه در $K[x]$ است (نتیجهٔ III ۴۰۶۰)، $c^{-1}f$ تکین‌است، و $(f) = (c^{-1}f)$ (قضیهٔ III ۲۰۳۰). درنتیجه، می‌توان فرض کرد f تکین است. بنابر قضیهٔ اول یکریختی (نتیجهٔ III ۱۰۰۲۰)،

$$K[x]/(f) = K[x]/\operatorname{Ker} \varphi \cong \operatorname{Im} \varphi = K[u].$$

چون $K[u]$ دامنه صحیح است، ایده‌آل (f)، طبق قضیهٔ III ۱۶۰۲۰، اول است. قضیهٔ III ۴۰۳۰ ایجاب می‌کند که f تحویل‌ناپذیر، و درنتیجه ایده‌آل (f) ماکزیمال، باشد. درنتیجه، $K[x]/(f)$ میدان می‌باشد (قضیهٔ III ۲۰۰۲). چون $K(u)$ کوچکترین زیرمیدانی از F است که‌شامل K و u است و نیز $K(u) \supset K[u] \cong K[x]/(f)$، باید داشته باشیم $K(u) = K[u]$. یکتایی f از تکین بودن آن و اینکه

$$g(u) = 0 \iff g \in \operatorname{Ker} \varphi = (f) \iff f,\ g \text{ را عاد می‌کند}$$

نتیجه می‌شود.

(چهار) بنابرقضیهٔ ۳.۱، هرعنصر $g \in K[x]$ به‌ازای $K(u) = K[u]$ ای به شکل $g(u)$ است. الگوریتم تقسیم نشان می‌دهد که $g = qf + h$، که در آن $q, h \in K[x]$ و $\deg h < \deg f$. بنابراین،

$$g(u) = q(u) f(u) + h(u) = 0 + h(u) = h(u) = b_0 + b_1 u + \cdots + b_m u^m$$

که در آن $m < n = \deg f$. لذا، $\{1_K, u, \ldots, u^{n-1}\}$، K ــ فضای برداری $K(u)$ را می‌پیماید. برای مشاهدهٔ استقلال خطی $\{1_K, u, \ldots, u^{n-1}\}$ روی K، و درنتیجه پایه بودن آن، فرض کنیم

$$a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = 0 \qquad (a_i \in K).$$

در این صورت، $g = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in K[x]$ دارای u به عنوان ریشه بوده و درجهٔ نابیشتر از $n - 1$ دارد. چون طبق (دو) $f \mid g$ و $\deg f = n$، باید داشته باشیم $g = 0$؛ یعنی، به‌ازای هر i، $a_i = 0$، که از آنجا $\{1_K, u, \ldots, u^{n-1}\}$ مستقل خطی می‌باشد. لذا، $\{1_K, u, \ldots, u^{n-1}\}$ یک پایه از $K(u)$ است.

(سه) نتیجهٔ فوری (چهار) است. معادل بودن (چهار) و (پنج) تمرینی عادی خواهد بود.

تعریف ۷.۱. فرض کنیم F یک توسیع میدان K بوده و $u \in F$ روی K جبری باشد. چندجمله‌ای تحویل‌ناپذیر تکین f در قضیهٔ ۶.۱ **چندجمله‌ای تحویل‌ناپذیر** (یا **مینیمال** یا **مینیمم**) u نام دارد. **درجهٔ u روی K** عبارت است از $\deg f = [K(u) : K]$.

مثال زیر طرز استفاده از قضیهٔ ۶.۱ و تکنیکهای برهانش در محاسباتی خاص را نشان می‌دهد.

مثال. چندجمله‌ای $x^3 - 3x - 1$ روی $\mathbf{Q}$ تحویل‌ناپذیر است (قضیهٔ III ۶.۶۰ و حکم III ۸.۶۰) و دارای ریشهٔ حقیقی u می‌باشد (تمرین III ۱۶.۶۰ (ت)). بنابر قضیهٔ ۶.۱، u دارای درجهٔ 3 روی $\mathbf{Q}$ است و $\{1, u, u^2\}$ پایه‌ای از $\mathbf{Q}(u)$ روی $\mathbf{Q}$ دارد. عنصر $u^4 + 2u^3 + 3 \in \mathbf{Q}(u) = \mathbf{Q}[u]$ را می‌توان به صورت ترکیبی خطی از عناصر پایه (روی $\mathbf{Q}$) به‌صورت زیر بیان کرد. الگوریتم تقسیم (یعنی، تقسیم طولانی معمولی) در حلقهٔ $\mathbf{Q}[x]$

نشان می‌دهد که

$$x^4 + 2x^3 + 3 = (x + 2)(x^3 - 3x - 1) + (3x^2 + 7x + 5),$$

که از آنجا

$$\begin{aligned} u^4 + 2u^3 + 3 &= (u + 2)(u^3 - 3u - 1) + (3u^2 + 7u + 5) \\ &= (u + 2)0 + (3u^2 + 7u + 5) \\ &= 3u^2 + 7u + 5. \end{aligned}$$

معکوس ضربی چندجمله‌ای $3u^2 + 7u + 5$ در $\mathbf{Q}(u)$ را می‌توان به‌صورت زیر حساب کرد. چون $x^3 - 3x - 1$ و $3x^2 + 7x + 5$ در $\mathbf{Q}[x]$ تحویل‌ناپذیر است، چندجمله‌ایهای $g(x), h(x) \in \mathbf{Q}[x]$، ۱۱.۳۰ III در $\mathbf{Q}[x]$ نسبت به هم اولند. درنتیجه، طبق قضیهٔ ۱۱.۳۰ III ای وجود دارند به‌طوری‌که

$$(x^3 - 3x - 1)g(x) + (3x^2 + 7x + 5)h(x) = 1.$$

بنابراین، چون $u^3 - 3u - 1 = 0$، داریم

$$(3u^2 + 7u + 5)h(u) = 1.$$

درنتیجه، $h(u) \in \mathbf{Q}[u]$ معکوس $3u^2 + 7u + 5$ است. چندجمله‌ایهای g و h را می‌توان به وسیلهٔ الگوریتم اقلیدسی (تمرین ۱۳.۳۰ III) صریحاً حساب کرد: $g(x) = -7/37x + 29/111$ و $h(x) = 7/111\ x^2 - 26/111\ x + 28/111$. از بنابراین، $h(u) = 7/111\ u^2 - 26/111\ u + 28/111$.

فرض کنیم E یک توسیع میدان F، K یک توسیع میدان L، و $\sigma : K \to L$ یک یکریختی میدانها باشد. سئوالی که مکرر در بررسی توسیعهای میدان مطرح می‌شود این است که تحت چه شرایطی می‌توان σ را به یک یکریختی E به روی F توسیع داد. به عبارت دیگر، آیا یک یکریختی مانند $\tau : E \to F$ هست که $\tau \mid K = \sigma$؟ حال به این سوال به‌ازای توسیعهای میدان ساده جواب می‌دهیم و در این کار محکهایی برای آنکه دو توسیع سادهٔ $K(u)$ و $K(v)$ یکریخت باشند به دست می‌آوریم (همچنین، ر.ک. تمرین ۱۶).

به یاد آورید که هرگاه $\sigma : R \to S$ یک یکریختی حلقه‌ها باشد، آنگاه نگاشت $R[x] \to S[x]$ داده شده با $\sum_i r_i x^i \mapsto \sum_i \sigma(r_i)x^i$ نیز یک یکریختی حلقه‌هاست (تمرین ۱.۵۰ III). واضح است که این نگاشت σ را توسیع می‌بخشد. ما نگاشت توسیع یافتهٔ

$R[x] \to S[x]$ را نیز با σ و نقش $f \in R[x]$ را با σf نشان می‌دهیم.

قضیهٔ ۸.۱. *فرض کنیم $\sigma : K \to L$ یک‌یکریختی میدانها، u عنصری از توسیع میدان K، و v عنصری از توسیع میدان L باشد. همچنین،*
(یک) u روی K و v روی L متعالی باشند؛ یا
(دو) u ریشه‌ای از چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ و v ریشه‌ای از $\sigma f \in L[x]$ باشد.
دراین‌صورت، σ به یک یکریختی میدانها مانند $K(u) \cong L(v)$ توسیع می‌یابد که u را به v می‌نگارد.

طرح برهان. (یک) بنابرتبصره‌های‌قبل‌ازقضیه، σ به یک یکریختی مانند $K[x] \cong L[x]$ توسیع می‌یابد. تحقیق کنید این نگاشت به یک‌یکریختی $K(x) \to L(x)$ داده شده با $h/g \mapsto \sigma h/\sigma g$ توسیع می‌یابد. بنابراین، طبق قضیهٔ ۵.۱، داریم $K(u)K(x) \cong L(x) \cong L(u)$. نگاشت مرکب σ را توسیع بخشیده و u را به v می‌نگارد.

(دو) کافی است فرض کنیم f تکین است. چون $\sigma : K[x] \cong L[x]$، این ایجاب می‌کند که $\sigma f \in L[x]$ تکین تحویل‌ناپذیر باشد. بنابر برهان قضیه ۶.۱، نگاشتهای

$$\varphi : K[x]/(f) \to K[u] = K(u) \quad \text{و} \quad \psi : L[x]/(\sigma f) \to L[v] = L(v),$$

که به ترتیب با $\varphi[g + (f)] = g(u)$ و $\psi[h + (\sigma f)] = h(v)$ داده می‌شوند، یکریختی‌اند. نگاشت $\theta : K[x]/(f) \to L[x]/(\sigma f)$ داده شده با $\theta[g + (f)] = \sigma g + (\sigma f)$، طبق نتیجهٔ III ۱۱.۲۰، یکریختی است. بنابراین، ترکیب

$$K(u) \xrightarrow{\varphi^{-1}} K[x]/(f) \xrightarrow{\theta} L[x]/(\sigma f) \xrightarrow{\psi} L(v)$$

یک یکریختی میدانهاست به‌طوری‌که $g(u) \mapsto (\sigma g)(v)$. بخصوص، $\psi\theta\varphi^{-1}$ با σ بر K یکی است و u را به v می‌نگارد (چون طبق تمرین III ۱۵.۱۰، $\sigma(1_K) = 1_L$).

نتیجهٔ ۹.۱. *فرض کنیم E و F هریک توسیعهای میدان K بوده و $u \in E$ و $v \in F$ روی K جبری باشند. دراین صورت، u و v ریشه‌های چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ اند اگر و فقط اگر یک یکریختی میدانها مانند $K(u) \cong K(v)$ وجود داشته باشد که u را به v برده و بر K همانی باشد.*

برهان. ($\Leftarrow$) قضیهٔ ۸.۱.۱ را به‌ازای $\sigma = 1_K$ به‌کار برید (درنتیجه، به‌ازای هر $f \in K[x]$، $\sigma f = f$).

($\Rightarrow$) فرض کنیم $\sigma : K(u) \cong K(v)$، که در آن $\sigma(u) = v$، و، به‌ازای هر $k \in K$، $\sigma(k) = k$. فرض کنیم $f \in K[x]$ چندجمله‌ای تحویل‌ناپذیر مربوط به عنصر جبری u باشد. هرگاه $f = \sum_{i=0}^{n} k_i x^i$، آنگاه $0 = f(u) = \sum_{i=0}^{n} k_i u^i$. بنابراین،

$$0 = \sigma\left(\sum_{i=0}^{n} k_i u^i\right) = \sum_i \sigma(k_i u^i) = \sum_i \sigma(k_i)\sigma(u^i) = \sum_i k_i \sigma(u)^i = \sum_{i=0}^{n} k_i v^i = f(v).$$

تا اینجا همواره با ریشهٔ چندجمله‌ای $f \in K[x]$ در توسیع میدان داده شدهٔ F از K سروکارداشته‌ایم. قضیهٔ زیرنشان می‌دهد که واقعاً لازم نیست F از پیش معلوم باشد.

قضیهٔ ۱۰.۱. *هرگاه K میدان و $f \in K[x]$ یک‌چندجمله‌ای از درجهٔ n باشد، آنگاه یک توسیع میدان ساده مانند $F = K(u)$ از K وجود دارد به‌طوری‌که*

(یک) $u \in F$ ریشه‌ای از f است؛

(دو) $[K(u) : K] \leq n$، که در آن تساوی برقرار است اگر و فقط اگر f در $K[x]$ تحویل‌ناپذیر باشد؛

(سه) هرگاه f در $K[x]$ تحویل‌ناپذیر باشد، آنگاه $K(u)$ با تقریب یکریختی که بر K همانی است منحصر به فرد است.

تبصره. در پرتو (سه) معمولاً میدان F حاصل از *الحاق یک ریشهٔ* چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ به میدان K صحبت می‌شود.

طرح برهان ۱.۱.۱. می‌توان فرض کرد f تحویل‌ناپذیر است (در صورت نبودن، f را با یکی از عوامل تحویل ناپذیرش عوض می‌کنیم). دراین صورت، ایده‌آل (f) در $K[x]$ ماکزیمال است (قضیهٔ ۴.۳.۰ III ونتیجهٔ ۴.۶.۰ III) وحلقهٔ خارج قسمتی $F = K[x]/(f)$ یک میدان می‌باشد (قضیهٔ ۲.۰.۲ III). به علاوه، تصویر کانونی $\pi : K[x] \to K[x]/(f) = F$؛ وقتی به K تحدید می‌شود، یک تکریختی است (زیرا ۰ تنها ثابت در ایده‌آل ماکزیمال $K[x]$ است). لذا، F شامل $\pi(K) \cong K$؛ ولذا، می‌توان آن را به صورت یک توسیع میدان K (مشروط بر اینکه K با $\pi(K)$ تحت یکریختی یکی شده باشد) درنظر گرفت. به‌ازای

$x \in K[x]$ ، فرض کنید $u = \pi(x) \in F$. تحقیق کنید که $F = K(u)$ و $f(u) = 0$ در F . قضیهٔ ۶۰۱ حکم (دو) و نتیجهٔ ۹۰۱ قسمت (سه) را ایجاب می‌کند .

تا پایان این بخش، به ارائهٔ مطالب اساسی در باب توسیعهای میدان جبری می‌پردازیم .

قضیهٔ ۱۱۰۱ . هرگاه F یک توسیع میدان با بعد متناهی از K باشد ، آنگاه F روی K با تولید متناهی و جبری است .

برهان . هرگاه $[F : K] = n$ و $u \in F$ ، آنگاه مجموعهٔ $n+1$ عنصری $\{1_K, u, u^2, \ldots, u^n\}$ باید وابستهٔ خطی باشد . از اینرو ، $a_i \in K$ هایی وجود دارند ، که همه صفر نیستند ، به طوری‌که $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$ ، که‌ایجاب می‌کند که u روی K جبری باشد . چون u دلخواه بود ، F روی K جبری است . هرگاه $\{v_1, \ldots, v_n\}$ پایه‌ای از F روی K باشد ، آنگاه به‌آسانی معلوم می‌شود که $F = K(v_1, \ldots, v_n)$.

قضیهٔ ۱۲۰۱ . هرگاه F یک توسیع میدان K بوده و X زیرمجموعه‌ای از F باشد به طوری‌که $F = K(X)$ و هر عنصر X روی K جبری باشد ، آنگاه F یک توسیع جبری K می‌باشد . هرگاه X مجموعه‌ای متناهی باشد ، آنگاه F روی K با بعد متناهی می‌باشد .

برهان . هرگاه $v \in F$ ، آنگاه به‌ازای $u_i \in X$ ی ، $v \in K(u_1, \ldots, u_n)$ (قضیهٔ ۳۰۱) و زنجیری از زیرمیدانها وجود دارد :

$$K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, \ldots, u_{n-1}) \subset K(u_1, \ldots, u_n).$$

چون u_i روی K جبری است ، به‌ازای هر $i \geq 2$ ، لزوماً " روی $K(u_1, \ldots, u_{i-1})$ جبری است ؛ مثلاً " ، از درجهٔ r_i . چون $K(u_1, \ldots, u_{i-1})(u_i) = K(u_1, \ldots, u_i)$ ، طبق قضیهٔ ۶۰۱ داریم $[K(u_1, \ldots, u_i) : K(u_1, \ldots, u_{i-1})] = r_i$. فرض کنیم r_1 درجهٔ u_1 روی K باشد ؛ در این‌صورت ، کاربرد مکرر قضیهٔ ۲۰۱ نشان می‌دهد که $[K(u_1, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$. بنابر قضیهٔ ۱۱۰۱ ، $K(u_1, \ldots, u_n)$ (و درنتیجه ، v) روی K جبری است . چون $v \in F$ دلخواه بود ، F روی K جبری می‌باشد . اگر $X = \{u_1, \ldots, u_n\}$ متناهی باشد ، همین برهان (به‌ازای $F = K(u_1, \ldots, u_n)$) نشان می‌دهد که $[F : K] = r_1 r_2 \cdots r_n$ متناهی می‌باشد .

قضیهٔ ۱۴۰۱ . هرگاه F توسیع میدان جبری E و E توسیع میدان جبری K باشد ، آنگاه F توسیع جبری K می‌باشد .

برهان . فرض‌کنیم $u \in F$ ؛ چون u روی E جبری‌است ، به‌ازای $b_i \in E$ هایی $(b_n \neq 0)$ ، $b_n u^n + \cdots + b_1 u + b_0 = 0$. بنابراین ، u روی زیرمیدان $K(b_0, \ldots, b_n)$ جبری است . درنتیجه ، زنجیری از میدانها مانند

$$K \subset K(b_0, \ldots, b_n) \subset K(b_0, \ldots, b_n)(u)$$

وجود دارد ، که‌در آن $[K(b_0, \ldots, b_n)(u) : K(b_0, \ldots, b_n)]$ بنابر قضیهٔ ۶۰۱ متناهی است (زیرا u روی $K(b_0, \ldots, b_n)$ جبری‌است) و $[K(b_0, \ldots, b_n) : K]$ بنابرقضیهٔ ۱۲۰۱ متناهی است (زیرا هر $b_i \in E$ روی K جبری است) . بنابراین ، $[K(b_0, \ldots, b_n)(u) : K]$ متناهی می‌باشد (قضیهٔ ۲۰۱) . از اینرو ، $u \in K(b_0, \ldots, b_n)(u)$ روی K جبری‌خواهد بود (قضیهٔ ۱۱۰۱) . چون u دلخواه بود ، F روی K جبری می‌باشد .

قضیهٔ ۱۴۰۱ . فرض‌کنیم F یک توسیع میدان K بوده و E مجموعهٔ تمام عناصر F باشد که روی K جبری‌اند . در این‌صورت ، E زیرمیدانی از F است (که ، البته ، روی K جبری است) .

واضح است که زیرمیدان E توسیع جبری ماکزیمال منحصر به فردی از K است که مشمول F می‌باشد .

برهان ۱۴۰۱. هرگاه $u, v \in E$ ، آنگاه ، بنابر قضیهٔ ۱۲۰۱ ، $K(u,v)$ یک توسیع جبری میدان K است . لذا ، چون $u - v$ و uv^{-1} $(v \neq 0)$ در $K(u,v)$ اند ، $u - v$ و uv^{-1} در E می‌باشند . این ایجاب می‌کند که E میدان باشد (ر.ک. قضیهٔ ۵۰۲۰ I) .

ضمیمه: ترسیم با خط‌کش و پرگار

واژهٔ "خط‌کش" مترادف ستاره است (که در بحثهای هندسی مصطلح است) . با استفاده از توسیعهای میدان ، دو مسئلهٔ مشهور قدیمی را سامان می‌دهیم :

(آ) آیا می‌توان با خط‌کش و پرگار یک زاویهٔ دلخواه را سه قسمت کرد ؟

(ب) آیا می‌توان با خط کش و پرگار یک مکعب را مضاعف ساخت (یعنی، ضلع مکعبی را رسم کرد که حجمش دو برابر حجم مکعب داده شده باشد)؟

فرض این است که تمام ترسیمات با خط‌کش و پرگار که در اغلب کتب هندسهٔ مسطحه می‌آیند را بدانیم. مثال: به‌ازای خط مستقیم L و نقطهٔ P غیرواقع بر آن، خط مستقیم منحصر به فردی از P به موازات L [عمود بر L] قابل رسم است. در اینجا و ذیلا "قابل رسم" یعنی "قابل رسم با خط‌کش و پرگار."

به علاوه، دیدگاه هندسهٔ تحلیلی را به صورت زیر می‌پذیریم. واضح است که می‌توان با خط‌کش و پرگار دو خط مستقیم عمود بر هم (محورها) رسم کرد. طول یکه‌ای اختیار می‌کنیم. در این صورت، می‌توان تمام نقاط صفحه به مختصات صحیح را رسم کرد (یعنی، آنها را به عنوان اشتراک خطوط مستقیم رسم‌پذیری موازی محورها مشخص کرد). بزودی خواهیم دید که مسائل ذکر شده از معلومات ما از اینکه چه نقاط دیگری در صفحه با خط‌کش و پرگار رسم‌پذیرند نتیجه می‌شوند.

اگر F زیرمیدانی از میدان اعداد حقیقی $\mathbf{R}$ باشد، **صفحهٔ** F زیرمجموعه‌ای از صفحه می‌باشد که مرکب از تمام نقاط (c,d) است که $c \in F, d \in F$. اگر P,Q نقاط متمایزی در صفحهٔ F باشند، خط منحصر به فرد مار بر P و Q یک **خط در** $\mathbf{F}$ نام دارد، و دایره به مرکز P وشعاع پاره‌خط PQ یک **دایره در** $\mathbf{F}$ نامیده می‌شود. به آسانی تحقیق می‌شود که هر خط مستقیم در F معادله‌ای به شکل $ax + by + c = 0$ $(a,b,c \in F)$ دارد، و هر دایره در F معادله‌ای به شکل $x^2 + y^2 + ax + by + c = 0$ $(a,b,c \in F)$ خواهد داشت (تمرین ۲۴).

لم ۱۵۰۱. *فرض کنیم F زیرمیدانی از میدان اعداد حقیقی R بوده و L_1,L_2 خطوطی غیرموازی در F و C_1,C_2 دوایری متمایز در F باشند. در این صورت،*

(یک) $L_1 \cap L_2$ نقطه‌ای در صفحهٔ F است؛

(دو) $L_1 \cap C_1 = \varnothing$ یا از یک یا دو نقطه در صفحهٔ $F(\sqrt{u})$ به‌ازای $u \in F$ ای $(u \geq 0)$ تشکیل شده است.

(سه) $C_1 \cap C_2 = \varnothing$ یا از یک یا دو نقطه در صفحهٔ $F(\sqrt{u})$ به‌ازای $u \in F$ ای $(u \geq 0)$ تشکیل شده است.

طرح برهان. (یک) تمرین. (سه) اگر دوایر عبارت باشند از

$$C_1 : x^2 + y^2 + a_1x + b_1y + c_1 = 0 \quad \text{و} \quad C_2 : x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

(بنابر نکات پیش از لم، $a_i,b_i,c_i \in F$)، نشان دهید که $C_1 \cap C_2$ همان اشتراک C_1 یا C_2 با خط مستقیم $L : (a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$ است. تحقیق کنید که L یک خط در F است؛ در این صورت، حالت (سه) به حالت (دو) تحویل می‌یابد.

(دو) فرض کنیم L_1 به معادلهٔ $dx + ey + f = 0$ $(d,e,f \in F)$ باشد. حالت $d = 0$ به عنوان تمرین می‌ماند؛ اگر $d \neq 0$، می‌توان فرض کرد $d = 1$ (چرا؟)؛ درنتیجه، $x = (-ey - f)$. هرگاه $(x,y) \in L_1 \cap C_1$، آنگاه جانشانی معادلهٔ C_1 را به صورت $(-ey - f)^2 + y^2 + a_1(-ey - f) + b_1y + c_1 = Ay^2 + By + C = 0$ به دست می‌دهد، که در آن $A,B,C \in F$. هرگاه $A = 0$، آنگاه $y \in F$؛ از اینرو، $x \in F$ و $x,y \in F(\sqrt{1}) = F$. اگر $A \neq 0$، می‌توان فرض کرد $A = 1$. در این صورت، $y^2 + By + C = 0$ و کامل‌کردن مربعات نتیجه می‌دهد که $(y + B/2)^2 + (C - B^2/4) = 0$. این ایجاب می‌کند که $L_1 \cap C_1 = \varnothing$ یا $x,y \in F(\sqrt{u})$ که $u = -C + B^2/4 \geq 0$.

گوییم عدد حقیقی c **رسم‌پذیر** است اگر نقطهٔ $(c,0)$ را بتوان با دنباله‌ای متناهی از ترسیمات به وسیلهٔ خط‌کش و پرگار که با نقاط به مختصات صحیح شروع می‌شوند رسم کرد (دقیقاً" مشخص نمود). واضح است که رسم‌پذیری c (یا $(c,0)$) معادل رسم‌پذیری (به وسیلهٔ خط‌کش و پرگار) یک پاره‌خط به طول $|c|$ است. به علاوه، نقطهٔ (c,d) در صفحه را می‌توان به وسیلهٔ خط‌کش و پرگار رسم کرد اگر و فقط اگر هر دوی c و d اعداد حقیقی رسم‌پذیری باشند. واضح است که اعداد صحیح رسم‌پذیرند، و اثبات مطالب زیر مشکل نمی‌باشد (ر.ک. تمرین ۲۵):

(یک) هر عدد گویا رسم‌پذیر است؛

(دو) اگر $c \geq 0$ رسم‌پذیر باشد، $\sqrt{c}$ نیز چنین است؛

(سه) هرگاه c,d رسم‌پذیر باشند، آنگاه $c \pm d$، cd، و c/d $(d \neq 0)$ رسم‌پذیرند؛

درنتیجه، اعداد رسم‌پذیر زیرمیدانی از اعداد حقیقی تشکیل می‌دهند که شامل اعداد گویا می‌باشد.

حکم ۱۶.۱. هرگاه عدد حقیقی c رسم‌پذیر باشد، آنگاه c روی میدان اعداد گویای

$\mathbf{Q}$ جبری و درجه‌اش توانی از 2 می‌باشد.

برهان. نکات فوق نشان می‌دهند که صفحهٔ $\mathbf{Q}$ را نیز می‌شود در نظر گرفت. در این صورت، رسم پذیری c یعنی $(c,0)$ را می‌توان با دنباله‌ای متناهی از ترسیمات مجاز به وسیلهٔ خط‌کش و پرگار که از صفحهٔ $\mathbf{Q}$ آغاز می‌شوند مشخص (رسم) کرد. در جریان این ترسیمات نقاط مختلف صفحه به عنوان اشتراک خطوط و/یا دوایر به کار رفته در فرایند ترسیم معین می‌شوند. این تنها راه رسیدن به نقاط جدید فقط با خط‌کش و پرگار است. قدم اول در فرایند رسم خط یا دایره است، که هر یک از آنها کاملا" با دو نقطه (مرکز P و شعاع PT برای دایره) معین می‌شود. یا این نقاط در صفحهٔ $\mathbf{Q}$ داده شده‌اند یا می‌توان آنها را دلخواه گرفت، که در این حالت نیز می‌توانند در صفحهٔ $\mathbf{Q}$ اختیار شوند. به همین نحو، در هر مرحله از ترسیم، دو نقطهٔ معین کنندهٔ خط یا دایره را می‌توان نقاطی در صفحهٔ $\mathbf{Q}$ یا نقاطی که در مراحل قبل رسم شده‌اند گرفت. در پرتو لم ۱۵۰۱، اولین نقطهٔ جدید رسم شده به این صورت در صفحهٔ توسیع میدان $\mathbf{Q}(\sqrt{u})$ از $\mathbf{Q}$ قرار دارد، که $u \in \mathbf{Q}$، یا معادلا" در صفحهٔ توسیع $\mathbf{Q}(v)$ که $v^2 \in \mathbf{Q}$ واقع می‌باشد. یک چنین توسیع دارای درجهٔ $2^0 = 1$ یا 2 روی $\mathbf{Q}$ (بسته به اینکه v در $\mathbf{Q}$ باشد یا نه) می‌باشد. به همین نحو، نقطهٔ جدید بعدی رسم شده در صفحهٔ $\mathbf{Q}(v,w) = \mathbf{Q}(v)(w)$ قرار دارد که $w^2 \in \mathbf{Q}(v)$. پس نتیجه می‌شود که یک دنبالهٔ متناهی از ترسیمات به وسیلهٔ خط‌کش و پرگار زنجیری متناهی از میدانهای زیر را به دست می‌دهد:

$$\mathbf{Q} \subset \mathbf{Q}(v_1) \subset \mathbf{Q}(v_1,v_2) \subset \cdots \subset \mathbf{Q}(v_1, \ldots, v_n)$$

که در آن $v_i^2 \in \mathbf{Q}(v_1, \ldots, v_{i-1})$ و $[\mathbf{Q}(v_1, \ldots, v_i) : \mathbf{Q}(v_1, \ldots, v_{i-1})] = 1$ یا مساوی 2 است $(2 \leq i \leq n)$. پس نقطهٔ $(c,0)$ رسم شده با این فرایند در صفحهٔ $F = \mathbf{Q}(v_1, \ldots, v_n)$ قرار دارد. بنابر قضیهٔ ۲۰۱، $[F : \mathbf{Q}]$ توانی از دو است. بنابراین، c روی $\mathbf{Q}$ جبری است (قضیهٔ ۱۱۰۱). اما $\mathbf{Q} \subset \mathbf{Q}(c) \subset F$ ایجاب می‌کند که $[\mathbf{Q}(c) : \mathbf{Q}]$، $[F : \mathbf{Q}]$ را عاد می‌کند (قضیهٔ ۲۰۱)، که از آنجا درجهٔ $[\mathbf{Q}(c) : \mathbf{Q}]$ از c روی $\mathbf{Q}$ توانی از 2 می‌باشد.

نتیجهٔ ۱۷۰۱. *زاویهٔ $60°$ را نمی‌توان با خط‌کش و پرگار به سه قسمت مساوی تقسیم کرد.*

برهان. اگر می‌توانستیم زاویهٔ $60°$ را سه قسمت کنیم، قادر به رسم مثلث قائمی با یک

زاویهٔ حادهٔ $20°$ بودیم. پس رسم عدد حقیقی (نسبت) $\cos 20°$ ممکن می‌بود (تمرین ۲۵). اما، مثلثات مقدماتی می‌گوید که، به‌ازای هر زاویهٔ α،

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

لذا، هرگاه $\alpha = 20°$، آنگاه $\cos 3\alpha = \cos 60° = \frac{1}{2}$ و $\cos 20°$ ریشهٔ معادلهٔ $8x^3 - 6x - 1 = 4x^3 - 3x = \frac{1}{2}$، و درنتیجه ریشهٔ چندجمله‌ای $8x^3 - 6x - 1$، می‌باشد. اما این چندجمله‌ای در $\mathbf{Q}[x]$ تحویل‌ناپذیر است (ر.ک. قضیهٔ III ۶۰۶۰ و حکم III ۸۰۶۰). بنابراین، طبق حکم ۱۶۰۱، $\cos 20°$ روی $\mathbf{Q}$ از درجهٔ 3 است و رسم‌پذیر نمی‌باشد.

نتیجهٔ ۱۸۰۱. *یک مکعب به ضلع 1 را نمی‌توان به وسیلهٔ خط‌کش و پرگار مضاعف ساخت (یعنی، ضلع مکعبی را رسم کرد که حجمش 2 باشد).*

برهان. هرگاه s طول یک ضلع مکعب به حجم 2 باشد، آنگاه s ریشهٔ $x^3 - 2$ است، که بنابر محک آیزنشتاین (قضیهٔ III ۱۵۰۶۰)، در $\mathbf{Q}[x]$ تحویل‌ناپذیر است. بنابراین، طبق حکم ۱۶۰۱، s ترسیم‌پذیر نیست.

تمرینات

تذکر. F همواره یک‌توسیع میدان از میدان K بوده و $\mathbf{Q},\mathbf{R},\mathbf{C}$ به ترتیب میدانهای اعداد گویا، حقیقی، و مختلط می‌باشند.

۱. (آ) $[F:K] = 1$ اگر و فقط اگر $F = K$.

(ب) هرگاه $[F:K]$ اول باشد، آنگاه هیچ میدان میانی بین F و K وجود ندارد.

(پ) هرگاه $u \in F$ از درجهٔ n روی K باشد، آنگاه n، $[F:K]$ را عاد می‌کند.

۲. یک توسیع میدان با تولید متناهی مثال بزنید که با بعد متناهی نباشد.
[**راهنمایی.** به متعالی فکر کنید.]

۳. هرگاه $u_1, \ldots, u_n \in F$، آنگاه میدان $K(u_1, \ldots, u_n)$ (یکریخت با) میدان خارج‌قسمتی حلقهٔ $K[u_1, \ldots, u_n]$ است.

۴. (آ) به‌ازای هر $u_1, \ldots, u_n \in F$ و هر جایگشت $\sigma \in S_n$،

$$K(u_1, \ldots, u_n) = K(u_{\sigma(1)}, \ldots, u_{\sigma(n)})$$

(ب) $K(u_1, \ldots, u_{n-1})(u_n) = K(u_1, \ldots, u_n)$.

(پ) مشابه‌های (آ) و (ب) را برای $K[u_1, \ldots, u_n]$ بیان و اثبات کنید.

(ت) هرگاه هر u_i روی K جبری باشد، آنگاه $K(u_1, \ldots, u_n) = K[u_1, \ldots, u_n]$.

۵. فرض کنید L و M زیرمیدانهایی از F بوده و LM ترکیب آنها باشد.

(آ) هرگاه $K \subset L \cap M$ و به‌ازای $S \subset M$ ی، $M = K(S)$، آنگاه $LM = L(S)$.

(ب) چه وقت LM اجتماع نظریهٔ مجموعه‌های $L \cup M$ است؟

(پ) اگر $E_1, \ldots, E_n$ زیرمیدانهایی از F باشند، نشان دهید که

$$E_1E_2\cdots E_n = E_1(E_2(E_3(\cdots(E_{n-1}(E_n)))\cdots).$$

۶. هر عنصر $K(x_1, \ldots, x_n)$ که در K نباشد روی K متعالی است.

۷. هرگاه v روی $K(u)$ به‌ازای $u \in F$ ای جبری بوده و v روی K متعالی باشد، آنگاه u روی $K(v)$ جبری می‌باشد.

۸. هرگاه $u \in F$ جبری و از درجهٔ فرد روی K باشد، آنگاه u^2 نیز چنین است و $K(u) = K(u^2)$.

۹. هرگاه $x^n - u \in K[x]$ تحویل‌ناپذیر بوده، $u \in F$ ریشه‌ای از $x^n - u$ باشد، و m، n راعادکند، آنگاه ثابت کنید درجهٔ u^m روی K مساوی n/m است. چندجمله‌ای تحویل‌ناپذیر مربوط به u^m روی K چیست؟

۱۰. هرگاه F روی K جبری بوده و D دامنهٔ صحیحی باشد به‌طوری‌که $K \subset D \subset F$، آنگاه D یک میدان است.

۱۱. (آ) یک توسیع میدان مانند $K \subset F$ مثال بزنید که $u, v \in F$ روی K متعالی باشند ولی $K(u,v) \not\cong K(x_1,x_2)$. [**راهنمایی.** v را روی میدان $K(u)$ درنظر بگیرید.]

(ب) قضیهٔ ۵.۱ را به n عنصرمتعالی $u_1, \ldots, u_n$ تعمیم‌داده و آن را ثابت کنید.

۱۲. اگر عدد صحیح $d \geq 0$ مربع نباشد، میدان $\mathbf{Q}(\sqrt{d})$ را توصیف کرده و مجموعهٔ عناصری که تمام میدان را تولید می‌کند را بیابید.

۱۳. (آ) توسیع $\mathbf{Q}(u)$ از $\mathbf{Q}$ رادرنظربگیریدکه‌باریشهٔ‌حقیقی u از $x^3 - 6x^2 + 9x + 3$ تولید می‌شود. (چرا این تحویل‌ناپذیر است؟) هر یک از عناصر $u^4; u^5; 3u^3 - u^4 + 2;\ (u+1)^{-1};\ (u^2 - 6u + 8)^{-1}$ رابرحسب پایهٔ $\{1, u, u^2\}$ بیان‌کنید.

(ب) همین کار را با پایهٔ $\{1, u, u^2, u^3, u^4\}$ از $\mathbf{Q}(u)$ انجام دهید، که در آن u ریشهٔ حقیقی $x^5 + 2x + 2$ است و عناصر مورد سوال عبارتند از

$$(u^2+2)(u^3+3u);\ u^{-1};\ u^4(u^4+3u^2+7u+5);\ (u+2)(u^2+3)^{-1}.$$

۱۴. (آ) اگر $F = \mathbf{Q}(\sqrt{2}, \sqrt{3})$، $[F : \mathbf{Q}]$ و یک پایهٔ F روی $\mathbf{Q}$ را بیابید.

(ب) همین کار را در مورد $F = \mathbf{Q}(i,\sqrt{3},\omega)$ انجام دهید، که در آن $i \in \mathbf{C}$، $i^2 = -1$، و ω ریشهٔ سوم (غیرحقیقی) مختلط ۱ است.

۱۵. درمیدان $K(x)$، فرض‌کنید $u = x^3(x+1)$. نشان‌دهید که $K(x)$ یک توسیع سادهٔ میدان $K(u)$ است. $[K(x) : K(u)]$ چیست؟

۱۶. در میدان $\mathbf{C}$، $\mathbf{Q}(i)$ و $\mathbf{Q}(\sqrt{2})$ به عنوان فضاهایی برداری یکریخت‌اند، ولی به عنوان میدان چنین نیستند.

۱۷. چندجمله‌ای تحویل‌ناپذیر f از درجهٔ 2 روی میدان Z_2 را بیابید. با الحاق ریشهٔ n از f به Z_2، میدان $Z_2(u)$ ازمرتبهٔ 4 رابه‌دست آورید. با همین روش، میدانی از مرتبهٔ 8 بسازید.

۱۸. گوییم یک عدد مختلط یک **عدد جبری** است اگر روی $\mathbf{Q}$ جبری باشد، و یک **عدد صحیح جبری** است اگر ریشهٔ یک چندجمله‌ای تکین در $\mathbf{Z}[x]$ باشد.

(آ) اگر u عددی جبری باشد، عدد صحیحی مانند n هست به‌طوری‌که nu یک عدد صحیح جبری است.

(ب) هرگاه $r \in \mathbf{Q}$ یک عدد صحیح جبری باشد، آنگاه $r \in \mathbf{Z}$.

(پ) هرگاه u یک عدد صحیح جبری بوده و $n \in \mathbf{Z}$، آنگاه $u+n$ و nu اعداد صحیح جبری می‌باشند.

(ت) مجموع و حاصلضرب دو عدد صحیح جبری اعداد صحیح جبری هستند.

۱۹. هرگاه $u,v \in F$ روی K جبری و به ترتیب از درجات m و n باشند، آنگاه $[K(u,v) : K] \leq mn$. هرگاه $(m,n) = 1$، آنگاه $[K(u,v) : K] = mn$.

۲۰. فرض کنید L و M میدانهایی میانی در توسیع $K \subset F$ باشند.

(آ) $[LM : K]$ متناهی است اگر و فقط اگر $[L : K]$ و $[M : K]$ متناهی باشند.

(ب) هرگاه $[LM : K]$ متناهی باشد، آنگاه $[L : K]$ و $[M : K]$، $[LM : K]$ را عاد می‌کنند و

$$[LM : K] \leq [L : K][M : K].$$

(پ) هرگاه $[L : K]$ و $[M : K]$ متناهی و نسبت به هم اول باشند، آنگاه

$$[LM : K] = [L : K][M : K].$$

(ت) هرگاه L و M روی K جبری باشند، آنگاه LM نیز چنین است.

۲۱. (آ) فرض کنید L و M میدانهایی میانی از توسیع $K \subset F$، با بعد متناهی روی

K ، باشند . همچنین ، $|LM:K] = [L:K][M:K]$ و ثابت کنید $L \cap M = K$.

(ب) عکس (آ) در صورتی که $[L:K]$ یا $[M:K]$ مساوی 2 باشد درست است .

(پ) با استفاده‌از یک ریشهٔ سوم حقیقی و یک ریشهٔ سوم غیرحقیقی 2 ، مثالی بزنید که در آن $[L:K] = [M:K] = 3$ ، $L \cap M = K$ ، ولی $[LM:K] < 9$.

۲۲ . F یک‌توسیع‌جبری K است‌اگرو فقط‌اگر ، به‌ازای هر میدان میانی E ، هر تکریختی $\sigma : E \to E$ که بر K همانی است یک خودریختی E باشد .

۲۳ . هرگاه $u \in F$ روی $K(X)$ به‌ازای $X \subset F$ ی جبری باشد ، آنگاه زیرمجموعه‌ای متناهی مانند $X' \subset X$ وجود دارد به‌طوری‌که u روی $K(X')$ جبری است .

۲۴ . فرض‌کنید F زیرمیدانی از $\mathbf{R}$ بوده و P,Q نقاطی در صفحهٔ اقلیدسی‌باشند که مختصاتشان‌در F قرار دارند .

(آ) خط مستقیم مار بر P و Q معادله‌ای به شکل $ax + by + c = 0$ دارد ، که در آن $a,b,c \in F$.

(ب) دایره به مرکز P و شعاع پاره‌خط PQ معادله‌ای به شکل

$$x^2 + y^2 + ax + by + c = 0$$

دارد ، که در آن $a,b,c \in F$.

۲۵ . فرض‌کنید c,d اعداد حقیقی رسم‌پذیری باشند .

(آ) $c + d$ و $c - d$ رسم‌پذیرند .

(ب) هرگاه $d \neq 0$ ، آنگاه c/d رسم‌پذیر است . [**راهنمایی.** هرگاه $(x,0)$ اشتراک محور x و خط مستقیم مار بر $(0,1)$ باشد که موازی خط مار بر $(0,d)$ و $(c,0)$ است ، آنگاه $x = c/d$.]

(پ) cd رسم‌پذیر است [**راهنمایی.** از قسمت (ب) استفاده کنید .]

(ت) اعداد حقیقی رسم‌پذیر یک زیرمیدان شامل $\mathbf{Q}$ تشکیل می‌دهند .

(ث) هرگاه $c \geq 0$ ، آنگاه $\sqrt{c}$ رسم‌پذیر است . [**راهنمایی.** هرگاه y طول پاره‌خط مستقیم عمود بر محور x باشد که $(1,0)$ را به (نیمهٔ بالایی) دایره به مرکز $((c+1)/2,0)$ و شعاع $(c+1)/2$ وصل می‌کند ، آنگاه $y = \sqrt{c}$.]

۲۶ . فرض‌کنید E_1 و E_2 زیرمیدانهایی‌از F بوده‌و X زیرمجموعه‌ای از F باشد . هرگاه هر عنصر E_1 روی E_2 جبری باشد ، آنگاه هر عنصر $E_1(X)$ روی $E_2(X)$ جبری است . [**راهنمایی .** $E_1(X) \subset (E_2(X))(E_1)$ ؛ از قضیهٔ ۱۲۰۱ استفاده کنید .]

۲ قضیهٔ اساسی

گروه گالوای یک توسیع میدان دلخواه را تعریف و مفهوم توسیع گالوا را برحسب گروه گالوا تعریف می‌کنیم. بقیهٔ بخش به اثبات قضیهٔ اساسی نظریهٔ گالوا (قضیهٔ ۵.۲) اختصاص دارد، که به ما توان بیان مسائل مربوط به میدانها، چندجمله‌ایها، و توسیعها را با اصطلاحات نظریهٔ گروهها می‌دهد. ضمیمهٔ آخر بخش به توابع گویای متقارن پرداخته و چند مثال از توسیعهایی که هر گروه متناهی داده شده را به عنوان گروه گالوا دارند به ما می‌دهد.

فرض کنیم F یک میدان باشد. مجموعهٔ $\operatorname{Aut} F$ مرکب از تمام خودریختیهای (میدان) $F \to F$ یک گروه تحت عمل ترکیب توابع تشکیل می‌دهند (تمرین ۱). این گروه در حالت کلی آبلی نیست. این کشف جالب گالوا بود که بسیاری از مسائل میدانها (بخصوص، در باب ریشه‌های چندجمله‌ایها روی میدان) درواقع با مسائلی در نظریهٔ گروهها درباب گروه خودریختی میدان معادلند. وقتی این مسائل مطرح می‌شوند، معمولاً نه فقط مستلزم F اند بلکه مستلزم یک زیرمیدان (مناسب اختیار شدهٔ) F نیز هستند؛ به عبارت دیگر، ما با توسیعهای میدان سر و کار خواهیم داشت.

اگر F یک توسیع میدان K باشد، در بخش ۱ دیدیم که ساختار K ــ مدول (فضای برداری) F اهمیت زیادی دارد. درنتیجه، طبیعی است آن خودریختیهایی از F را درنظر بگیریم که نگاشتهای K ــ مدولها نیز باشند. واضح است که مجموعهٔ تمام این خودریختیها زیرگروهی از $\operatorname{Aut} F$ است.

به‌طورکلی، فرض کنیم E و F توسیعهای میدان یک میدان مانند K باشند. هرگاه $\sigma : E \to F$ یک همریختی ناصفر از میدانها باشد، آنگاه، بنابر تمرین III ۱۵.۱۰، $\sigma(1_E) = 1_F$. هرگاه σ نیز یک همریختی K ــ مدولها باشد، آنگاه، به‌ازای هر $k \in K$،

$$\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_F = k.$$

به عکس، هرگاه یک‌همریختی میدانهای $\sigma : E \to F$، K را عنصروار ثابت بگذارد (یعنی، به‌ازای هر $k \in K$، $\sigma(k) = k$)، آنگاه σ ناصفر است و، به‌ازای هر $u \in E$،

$$\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$$

که از آنجا σ یک همریختی K ــ مدولها می‌باشد.

تعریف ۱۰.۲. فرض کنید E و F توسیعهای میدان یک میدان K باشند. نگاشت ناصفر

$\sigma : E \to F$ که هم‌همریختی میدانها و هم همریختی K ـ مدولها باشد یک **K ـ همریختی** نام دارد. به‌همین‌نحو، هرگاه یک خودریختی میدانها مانند $\sigma \in Aut\ F$ یک K ـ همریختی باشد، آنگاه σ یک **K ـ خودریختی** F است. گروه تمام K ـ خودریختیهای F **گروه گالوای** F روی K نام دارد و با $Aut_K F$ نموده می‌شود.

چند تبصره. K ـ تکریختیها و K ـ یکریختیها به‌نحو روشنی تعریف می‌شوند. در اینجا و در زیر، عنصر همانی $\mathrm{Aut}_K F$ و زیرگروه همانی آن هر دو با 1 نموده می‌شوند.

مثال. فرض کنیم $F = K(x)$، که در آن K میدان است. به‌ازای هر $a \in K$ که $a \neq 0$، نگاشت $\sigma_a : F \to F$ داده شده با $f(x)/g(x) \mapsto f(ax)/g(ax)$ یک K ـ خودریختی F است (این را می‌توان مستقیما" یا با نتایج III ۲۱۰۲۰ (چهار)، III ۶۰۴۰، و III ۶۰۵۰، و قضیهٔ III ۴۰۴۰ (دو) تحقیق کرد). هرگاه K نامتناهی باشد، آنگاه بی‌نهایت خودریختی متمایز σ_a وجود دارند، که از آنجا $\mathrm{Aut}_K F$ نامتناهی است. به همین نحو، به‌ازای هر $b \in K$، نگاشت $\tau_b : F \to F$ داده شده با $f(x)/g(x) \mapsto f(x+b)/g(x+b)$ یک K ـ خودریختی F است. هرگاه $a \neq 1_K$ و $b \neq 0$، آنگاه $\sigma_a \tau_b \neq \tau_b \sigma_a$، که از آنجا $\mathrm{Aut}_K F$ غیرآبلی است. همچنین، ر.ک. تمرین ۶.

قضیهٔ ۲۰۲. فرض کنیم F یک توسیع میدان K بوده و $f \in K[x]$. هرگاه $u \in F$ ریشه‌ای از f بوده و $\sigma \in Aut_K F$، آنگاه $\sigma(u) \in F$ نیز ریشه‌ای از f است.

برهان. هرگاه $f = \sum_{i=1}^{n} k_i x^i$، آنگاه $f(u) = 0$ ایجاب می‌کند که

$$0 = \sigma(f(u)) = \sigma(\sum k_i u^i) = \sum \sigma(k_i)\sigma(u^i) = \sum_i k_i \sigma(u)^i = f(\sigma(u)).$$

یکی از کاربردهای اصلی قضیهٔ ۲۰۲ در وضعیتی است که u روی K جبری بوده و چندجمله‌ای $f \in K[x]$ تحویل‌ناپذیر از درجهٔ n است. در این صورت، هر $\sigma \in \mathrm{Aut}_K K(u)$ کاملا" با عملش بر u معین می‌شود (زیرا، طبق قضیهٔ ۶۰۱، $\{1_K, u, u^2, \ldots, u^{n-1}\}$ پایه‌ای از $K(u)$ روی K است). چون $\sigma(u)$ طبق قضیهٔ ۲۰۲ ریشه‌ای از f است، $|\mathrm{Aut}_K K(u)| \leq m$،

که در آن m تعداد ریشه‌های متمایز f در $K(u)$ است (بنابر قضیهٔ III ۷۰۶۰ ، $m \leq n$) .

چند مثال . واضح است که هرگاه $F = K$ ، آنگاه $\mathrm{Aut}_K F$ فقط از عنصر همانی تشکیل شده است . اما عکس این مطلب درست نیست . مثلا" ، هرگاه u ریشهٔ سوم حقیقی 2 باشد (درنتیجه ، $\mathbf{Q} \subsetneq \mathbf{Q}(u) \subset \mathbf{R}$) ، آنگاه $\mathrm{Aut}_{\mathbf{Q}}\mathbf{Q}(u)$ گروه همانی است . زیرا تنها نقشهای ممکن u ریشه‌های $x^3 - 2$ اند و دو ریشهٔ دیگر مختلط می‌باشند . به همین نحو ، $\mathrm{Aut}_{\mathbf{Q}}\mathbf{R}$ همانی می‌باشد (تمرین ۲) .

چند مثال . $\mathbf{C} = \mathbf{R}(i)$ و $\pm i$ ریشه‌های $x^2 + 1$ اند . لذا ، $\mathrm{Aut}_{\mathbf{R}}\mathbf{C}$ مرتبه‌ای حداکثر 2 دارد . به‌آسانی تحقیق می‌شود که تزویج مختلط $(a + bi \mapsto a - bi)$ یک $\mathbf{R}$ ــ خودریختی همانی $\mathbf{C}$ است ؛ درنتیجه ، $|\mathrm{Aut}_{\mathbf{R}}\mathbf{C}| = 2$ ؛ ولذا ، $\mathrm{Aut}_{\mathbf{R}}\mathbf{C} \cong Z_2$. به همین نحو ، $\mathrm{Aut}_{\mathbf{Q}}\mathbf{Q}(\sqrt{3}) \cong Z_2$.

چند مثال . هرگاه $F = \mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2})(\sqrt{3})$ ، آنگاه چون $x^2 - 3$ روی $\mathbf{Q}(\sqrt{2})$ تحویل‌ناپذیر است ، برهان قضیهٔ ۲۰۱ و قضیهٔ ۶۰۱ نشان می‌دهد که $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ پایه‌ای از F روی $\mathbf{Q}$ است . لذا ، هرگاه $\sigma \in \mathrm{Aut}_{\mathbf{Q}}F$ ، آنگاه σ کاملا" توسط $\sigma(\sqrt{2})$ و $\sigma(\sqrt{3})$ معین می‌شود . بنابر قضیهٔ ۲۰۲ ، $\sigma(\sqrt{2}) = \pm\sqrt{2}$ و $\sigma(\sqrt{3}) = \pm\sqrt{3}$ و این یعنی حداکثر چهار $\mathbf{Q}$ ــ خودریختی از F وجود دارند . به آسانی تحقیق می‌شود که هر یک از چهار امکان عملا" یک $\mathbf{Q}$ ــ خودریختی F است و $\mathrm{Aut}_{\mathbf{Q}}F \cong Z_2 \oplus Z_2$.

در ضمیمه نشان داده شده‌است (حکم ۱۶۰۲) که به‌ازای هر گروه متناهی G ، یک توسیع باگروه‌گالوای G وجود دارد . هنوز به این سوال که آیا هر گروه متناهی گروه گالوای توسیعی روی یک میدان *خاص* (مانند $\mathbf{Q}$) هست یا نه جوابی یافت نشده است .

ایدهٔ اصلی آنچه معمولا" نظریهٔ گالوا خوانده می‌شود برقراری نوعی تناظر بین میدانهای‌میانی یک توسیع میدان مانند $K \subset F$ و زیرگروههای گروه گالوای $\mathrm{Aut}_K F$ است . با آنکه بیشترین توجه به حالتی است که F روی K با بعد متناهی است ، بحث را تاجایی که بتوانیم عام مطرح می‌کنیم . اولین گام در برقراری این تناظر را قضیهٔ زیر برمی‌دارد .

قضیهٔ ۳۰۲ . فرض کنیم F یک‌توسیع میدان K ، E یک‌میدان میانی ، و H یک زیرگروه $Aut_K F$ باشد . در این صورت ،

(یک) $H' = \{v \in F \mid \sigma(v) = v \text{ ، } \sigma \in H\}$ یک میدان میانی از توسیعهاست ؛

(دو) $E' = \{\sigma \in Aut_K F \mid \sigma(u) = u \text{ ، } u \in E\} = Aut_E F$ زیرگروه $Aut_K F$ می‌باشد .

برهان . تمرین .

میدان H' **میدان ثابت** H در F نام دارد (با آنکه این اصطلاحی متعارف است ، نماد عامی برای آن وجود ندارد ، ولی "نماد پریم" سودمندی‌اش ثابت می‌شود) . به همین نحو ، وقتی مناسب باشد ، در این محدوده گروه $Aut_K F$ را با E' نشان می‌دهیم . اگر $Aut_K F$ را با G نشان دهیم ، از یک سو به آسانی معلوم می‌شود که

$$F' = Aut\ F = 1 \quad \text{و} \quad K' = Aut_K F = G$$

و از سوی دیگر ، $1' = F$ (یعنی ، F میدان‌ثابت زیرگروه همانی است) . اما لزوماً درست نیست که $G' = K$ (و این را می‌توان در اولین مثال بعد از قضیهٔ ۳۰۲ دید ، که در آن $G = 1$ ؛ و درنتیجه ، $G' = F \neq K$ ؛ همچنین ، ر.ک. تمرین ۲) .

تعریف ۴۰۲ . فرض کنیم F یک‌توسیع میدان K باشد به‌طوری‌که‌میدان ثابت گروه گالوای $Aut_K F$ خود K باشد . در این صورت ، گوییم F یک **توسیع گالوای** (میدان) K است یا روی K **گالو** می‌باشد .[1]

---

۱ . یک توسیع گالوا اغلب بایدبا بعد متناهی یا دست‌کم جبری بوده و برحسب نرمالی و جدایی‌پذیری ،که دربخش ۳ مطرح خواهند شد ، تعریف شده باشد . در بعد متناهی ، تعریف ما با تعریف معمول معادل است . تعریف ما اساساً "از آرتین Artin است ، جز آنکه وی این نوع توسیع را "نرمال" می‌نامد . چون این مورد استعمال "نرمال" (در حالت $\text{char } F \neq 0$) با تعریف "نرمال" به‌کار رفته به وسیلهٔ بسیاری ازمولفان تداخل دارد ، ما روش اساسی آرتین را دنبال می‌کنیم ، ولی (بیش و کم) اصطلاح معمول را نگه خواهیم داشت .

چند تبصره. F روی K گالوا است اگر و فقط اگر به ازای هر $u \in F - K$ ، یک K ــ خودریختی مانند $\sigma \in \mathrm{Aut}_K F$ موجود باشد به طوری که $\sigma(u) \neq u$. هرگاه F یک توسیع میدان دلخواه K بوده و K_0 میدان ثابت $\mathrm{Aut}_K F$ باشد (احتمالا " $K_0 \neq K$) ، آنگاه به آسانی معلوم می‌شود که F روی K_0 گالوا است ، $K \subset K_0$ ، و $\mathrm{Aut}_K F = \mathrm{Aut}_{K_0} F$.

چند مثال. $\mathbf{C}$ روی $\mathbf{R}$ و $\mathbf{Q}(\sqrt{3})$ روی $\mathbf{Q}$ گالوا است (تمرین ۵) . هرگاه K یک میدان نامتناهی باشد ، آنگاه $K(x)$ روی K گالوا است (تمرین ۹) .

با آنکه هنوز ما با برهان فاصله داریم ، می‌توان قضیهٔ اساسی نظریهٔ گالوا را بیان کرد ؛ درنتیجه ، خواننده می‌تواند مسیر بحث را ببیند . اگر L و M میدانهای میانی یک توسیع با $L \subset M$ باشد ، بعد $[M : L]$ **بعد نسبی** L و M نامیده می‌شود . به همین نحو ، اگر H, J زیرگروههای گروه گالوا با $H < J$ باشند ، اندیس $[J : H]$ را **اندیس نسبی** H و J می‌نامند .

قضیهٔ ۵.۲ . (قضیهٔ اساسی نظریهٔ گالوا) . *هرگاه F یک توسیع گالوای با بعد متناهی K باشد ، آنگاه تناظر یک به یکی بین مجموعهٔ تمام میدانهای میانی توسیع و مجموعهٔ تمام زیرگروههای گروه گالوای $\mathrm{Aut}_K F$ (داده شده با $E \mapsto E' = \mathrm{Aut}_E F$) وجود دارد به طوری که*

(یک) بعد نسبی دو میدان میانی مساوی اندیس نسبی زیرگروه‌های نظیر است ؛ بخصوص ، $\mathrm{Aut}_K F$ دارای مرتبهٔ $[F : K]$ می‌باشد ؛

(دو) F روی هر میدان میانی E گالوا است ، ولی E روی K گالوا است اگر و فقط اگر زیرگروه نظیر $E' = \mathrm{Aut}_E F$ در $G = \mathrm{Aut}_K F$ نرمال باشد ؛ در این صورت ، G/E' با گروه گالوای $\mathrm{Aut}_K E$ ی E روی K مساوی (یکریخت) می‌باشد .

برهان قضیه (که در ص ۳۹۳ شروع می‌شود) به مقدماتی نسبتا " مفصل نیاز دارد . بقیهٔ این بخش به ذکر این مقدمات اختصاص دارد . مسئلهٔ ساختن توسیعهای میدان گالوا و توسیعهای گالوای جبری با ابعاد دلخواه را برای بخش بعد می‌گذاریم . خواننده باید توجه کند که بسیاری از احکامی که اکنون باید ثابت شوند در حالت کلی برقرارند .

همانطورکه درصورت‌قضیهٔ اساسی ذکر شد ، تناظر گالـــــــــــــوا با انتساب گروه گالوای $\mathrm{Aut}_E F$ ی F روی E به میدان میانی E داده می‌شود .خواهیم دید که معکوس این تناظریک به یک با انتساب میدان ثابت در F به‌زیرگروه H از گروه گالوا داده خواهد شد . شایسته‌است از "نماد پریم" قضیهٔ ۳.۲ استفاده کنیم ؛ درنتیجه ، E' مبین $\mathrm{Aut}_E F$ و H' مبین میدان ثابت H در F است .

مفید است این اعمال پریم‌گیری با شکل به صورت زیر تجسم شود . فرض کنیم L و M میـدانهای میـانی توسیع $K \subset F$ بوده و J,H زیرگروههای گروه گالوای $G = \mathrm{Aut}_K F$ باشند .

$$\begin{array}{ccc} F & \longmapsto & 1 \\ \cup & & \wedge \\ M & \longmapsto & M' \\ \cup & & \wedge \\ L & \longmapsto & L' \\ \cup & & \wedge \\ K & \longmapsto & G; \end{array} \qquad \begin{array}{ccc} F & \longmapsto & 1 \\ \cup & & \wedge \\ H' & \longmapsto & H \\ \cup & & \wedge \\ J' & \longmapsto & J \\ \cup & & \wedge \\ K & & G. \end{array}$$

به‌طور صوری ، مطالب اساسی در باب اعمال پریم‌گیری در لم زیر داده شده‌اند .

لم ۶.۲ . *فرض کنیم F یک‌توسیع میدان K با میدانهای‌میانی L و M باشند .همچنین ، H و J زیرگروههای $G = Aut_K F$ باشند . در این صورت ،*

(یک) $K' = G$ و $F' = 1$ ؛

(یک′) $1' = F$ ؛

(دو) $L \subset M \Rightarrow M' < L'$ ؛

(دو′) $H < J \Rightarrow J' \subset H'$ ؛

(سه) $L \subset L''$ و $H < H''$ *(که در آن* $L'' = (L')'$ و $H'' = (H')'$ *)* ؛

(چهار) $L' = L'''$ و $H' = H'''$.

طرح برهان. (یک) تا(سه) مستقیما" از تعاریف مناسبی نتیجه می‌شوند . برای اثبات قسمت اول (چهار) ، ملاحظه می‌شود که (سه) و (دو) ایجاب می‌کنند که $L''' < L'$ و از

(سه) با به‌کارگیری L' به‌جای H نتیجه می‌شود که $L' < L'''$. قسمت دیگر به همین نحو ثابت می‌شود .

چند تبصره. ممکن است L'' حقیقتا" شامل L باشد (به همین ترتیب در مورد H'' و H) . اگر $G' = K$ ، (طبق تعریف) F روی K گالواست . لذا ، چون در هر حال $K' = G$ ، F روی K گالواست اگر و فقط اگر $K = K''$. به همین نحو ، F روی میدان میانی E گالواست اگر و فقط اگر $E = E''$.

فرض کنیم X یک میدان میانی یا زیرگروه گروه گالوا باشد . X را **بسته** نامیم اگر $X = X''$. توجه کنید که F روی K گالواست اگر و فقط اگر K بسته باشد .

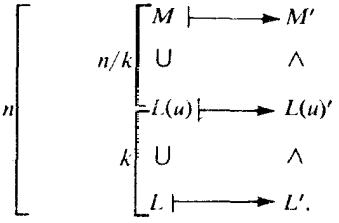
قضیهٔ ۷.۲ . *هرگاه F یک‌توسیع میدان K باشد ، آنگاه تناظر یک به یکی بین میدانهای میانی بستهٔ توسیع و زیرگروههای بستهٔ گروه گالوا وجود دارد ، که با $E \mapsto E' = Aut_E F$ داده شده است .*

برهان. تمرین؛ معکوس تناظر این‌طور داده می‌شود که به هر زیرگروه بستهٔ H میدان ثابت H' منتسب گردد . توجه کنید که ، طبق لم ۶.۲ (چهار) ، تمام اشیاء پریمدار بسته‌اند .

این قضیه تا وقتی اطلاعات بیشتری از میدانهای میانی و زیرگروههای بسته نداشته باشیم خیلی مفید نیست . مآلا" نشان می‌دهیم که ، در یک توسیع گالوای جبری ، تمام میدانهای میانی بسته‌اند و ، در بعد متناهی ، تمام زیرگروههای گروه گالوا نیز بسته می‌باشند . با چند لم تکنیکی شروع می‌کنیم تا ابعاد نسبی مختلف را تخمین بزنیم .

لم ۸.۲ . *فرض کنیم F توسیع میدان K بوده و L,M میدانهایی میانی باشند که $L \subset M$. هرگاه $[M : L]$ متناهی باشد ، آنگاه $[L' : M'] \leq [M : L]$. بخصوص ، هرگاه $[F : K]$ متناهی باشد ، آنگاه $|Aut_K F| \leq [F : K]$.*

برهان. به استقرا بر $n = [M : L]$ عمل می‌کنیم، که در آن حالت $n = 1$ بدیهی است. اگر $n > 1$ و قضیه به‌ازای هر $i < n$ درست باشد، $u \in M$ را طوری می‌گیریم که $u \notin L$. چون $[M : L]$ متناهی است، u روی L جبری (قضیهٔ ۱۱.۱) باچندجمله‌ای تحویل‌ناپذیر $f \in L[x]$ ازدرجهٔ $k > 1$ است. بنابر لمهای ۱۰۱ و ۶۰۱، $[L(u) : L] = k$ و $[M : L(u)] = n/k$. با تصویر داریم



اکنون دو حالت وجود دارد. هرگاه $k < n$، آنگاه $n/k < n$ و، به استقرا، $[L(u)' : M'] \leq n/k$ و $[L' : L(u)'] \leq k$. از اینرو،

$$[L' : M'] = [L' : L(u)'][L(u)' : M'] \leq k(n/k) = n = [M : L]$$

و قضیهٔ ثابت می‌شود. از آن سو، هرگاه $k = n$، آنگاه $[M : L(u)] = 1$ و $M = L(u)$. برای تکمیل برهان در این حالت، یک نگاشت انژکتیو از مجموعهٔ S تمام هم مجموعه‌های چپ M' در L' به مجموعهٔ T تمام ریشه‌های متمایز چندجمله‌ای $f \in L[x]$ (در F) می‌سازیم، که از آنجا $|T| \leq |S|$. چون، طبق قضیهٔ III ۷.۶.۰، $|T| \leq n$ و، طبق تعریف، $|S| = [L' : M']$، این نشان می‌دهد که $[L' : M'] \leq |T| \leq n = [M : L]$. در این صورت، حکم اخیر قضیه فورا" نتیجه می‌شود، زیرا $|\mathrm{Aut}_K F| = [\mathrm{Aut}_K F : 1] = [K' : F'] \leq [F : K]$.

فرض کنیم $\tau M'$ یک هم مجموعهٔ چپ M' در L' باشد. هرگاه $\sigma \in M' = \mathrm{Aut}_M F$، آنگاه چون $u \in M$، $\tau\sigma(u) = \tau(u)$. لذا، هر عنصر هم مجموعهٔ $\tau M'$ همین اثر را بر u دارد و خواهد نگاشت $u \mapsto \tau(u)$. چون $\tau \in L' = \mathrm{Aut}_L F$ و u ریشه‌ای از $f \in L[x]$ است، بنابر قضیهٔ ۲.۰.۲، $\tau(u)$ نیز ریشه‌ای از f می‌باشد. این ایجاب می‌کند که نگاشت $S \to T$ داده شده با $\tau M' \mapsto \tau(u)$ تعریف شده است. هرگاه $(\tau, \tau_0 \in L')$ $\tau(u) = \tau_0(u)$، آنگاه $\tau_0^{-1}\tau(u) = u$؛ و درنتیجه، $\tau_0^{-1}\tau$، u را ثابت نگه می‌دارد. بنابراین، $\tau_0^{-1}\tau$، $L(u) = M$ را عنصروار ثابت می‌گذارد (ر.ک. قضیهٔ ۶.۰.۱ (چهار)) و $\tau_0^{-1}\tau \in M'$. لذا، بنابر نتیجهٔ ۳.۴.۰.۱، $\tau_0 M' = \tau M'$، و نگاشت $S \to T$ انژکتیو است.

چند کاربرد مهم لم ۸۰۲ در ضمیمه مطرح شده‌اند. حال مشابه لم ۸۰۲ را برای زیرگروههای گروه گالوا ثابت می‌کنیم.

لم ۹۰۲. *فرض کنیم F یک توسیع میدان K بوده و H,J زیرگروههای گروه گالوای $Aut_K F$ باشند که $H < J$. هرگاه $[J : H]$ متناهی باشد، آنگاه $[H' : J'] \leq [J : H]$.*

برهان. فرض کنیم $n = [J : H]$ و $[H' : J'] > n$. در این صورت، عناصری مانند $u_1, u_2, \ldots, u_{n+1} \in H'$ وجود دارند که روی J' مستقل خطی‌اند. فرض کنیم $\{\tau_1, \tau_2, \ldots, \tau_n\}$ مجموعهٔ کاملی از نماینده‌های هم‌مجموعه‌های چپ H در J باشد (یعنی، $J = \tau_1 H \cup \tau_2 H \cup \cdots \cup \tau_n H$ و $\tau_i^{-1}\tau_j \in H$ اگر و فقط اگر $i = j$) و دستگاه n معادلهٔ خطی همگن از $n+1$ مجهول با ضرایب $\tau_i(u_j)$ در میدان F را درنظر می‌گیریم:

$$
\begin{aligned}
\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + \tau_1(u_3)x_3 + \cdots + \tau_1(u_{n+1})x_{n+1} &= 0\\
\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + \tau_2(u_3)x_3 + \cdots + \tau_2(u_{n+1})x_{n+1} &= 0\\
&\vdots\\
\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + \tau_n(u_3)x_3 + \cdots + \tau_n(u_{n+1})x_{n+1} &= 0
\end{aligned}
\qquad (1)
$$

این دستگاه همواره جواب نابدیهی دارد (یعنی، جوابی غیر از جواب صفر $x_1 = x_2 = \cdots = x_{n+1} = 0$؛ ر.ک. تمرین ۴۰۲۰ VII (ت)). در بین تمام این جوابهای نابدیهی یکی، مثلاً $x_1 = a_1, \ldots, x_{n+1} = a_{n+1}$، را با حداقل تعداد a_i های ناصفر اختیار می‌کنیم. با اندیسگذاری مجدد در صورت لزوم، می‌توان فرض کرد $(a_i \neq 0)$ $x_1 = a_1, \ldots, x_r = a_r, x_{r+1} = \cdots = x_{n+1} = 0$. چون هر مضرب یک جواب نیز جواب است، نیز می‌توان فرض کرد $a_1 = 1_F$ (اگر نبود، در a_1^{-1} ضرب می‌کنیم).

در زیر نشان می‌دهیم که فرض استقلال خطی $u_1, \ldots, u_{n+1} \in H'$ روی J' (یعنی، $[H' : J'] > n$) ایجاب می‌کند که $\sigma \in J$ ای وجود دارد به‌طوری‌که

$$x_1 = \sigma a_1, x_2 = \sigma a_2, \ldots, x_r = \sigma a_r, x_{r+1} = \cdots = x_{n+1} = 0$$

جوابی از دستگاه (۱) است و $\sigma a_2 \neq a_2$. چون تفاضل دو جواب نیز جواب است، $x_1 = a_1 - \sigma a_1, x_2 = a_2 - \sigma a_2, \ldots, x_r = a_r - \sigma a_r, x_{r+1} = \cdots = x_{n+1} = 0$ نیز یک جواب (۱) می‌باشد. اما چون $a_1 - \sigma a_1 = 1_F - 1_F = 0$ و $a_2 \neq \sigma a_2$، نتیجه می‌شود که

$x_1 = 0, x_2 = a_2 - \sigma a_2, \ldots, x_r = a_r - \sigma a_r, x_{r+1} = \cdots = x_{n+1} = 0$ یک جواب نابدیهی (۱) است $(x_2 \neq 0)$ با حداکثر $r-1$ درایهٔ ناصفر. این مینیمالی جواب $x_1 = a_1, \ldots, x_r = a_r, x_{r+1} = \cdots = x_{n+1} = 0$ را نقض می‌کند. بنابراین، طبق انتظار، $[H' : J'] \leq n$.

برای تکمیل برهان، باید $\sigma \in J$ را طوری بیابیم که خواص مطلوب را داشته باشد. اما، طبق تعریف، دقیقاً "یک τ_j، مثلاً τ_1، در H است"؛ بنابراین، به‌ازای هر i، $\tau_1(u_i) = u_i \in H'$. چون a_i ها یک جواب (۱) را تشکیل می‌دهند، معادلهٔ اول دستگاه نتیجه می‌دهد که

$$u_1a_1 + u_2a_2 + \cdots + u_ra_r = 0.$$

استقلال خطی u_i ها روی J' و ناصفربودن a_i ها ایجاب می‌کنند که a_i ی، مثلاً a_2، در J' نباشد. بنابراین، $\sigma \in J$ ای وجود دارد به‌طوری که $\sigma a_2 \neq a_2$.

حال دستگاه معادلات

$$\begin{aligned}
&\sigma\tau_1(u_1)x_1 + \sigma\tau_1(u_2)x_2 + \cdots + \sigma\tau_1(u_{n+1})x_{n+1} = 0\\
&\sigma\tau_2(u_1)x_1 + \sigma\tau_2(u_2)x_2 + \cdots + \sigma\tau_2(u_{n+1})x_{n+1} = 0\\
&\qquad\vdots\qquad\qquad\qquad\qquad\vdots\\
&\sigma\tau_n(u_1)x_1 + \sigma\tau_n(u_2)x_2 + \cdots + \sigma\tau_n(u_{n+1})x_{n+1} = 0
\end{aligned} \tag{۲}$$

را درنظر می‌گیریم. واضح است که، چون σ خودریختی بوده و

$$x_1 = a_1, \ldots, x_r = a_r, x_{r+1} = \cdots = x_{n+1} = 0$$

جوابی از (۱) است، $x_1 = \sigma a_1, \ldots, x_r = \sigma a_r, x_{r+1} = \cdots = x_{n+1} = 0$ جوابی از (۲) می‌باشد. حکم می‌کنیم که دستگاه (۲) جز در مورد ترتیب معادلات، با دستگاه (۱) یکی است (درنتیجه، $x_1 = \sigma a_1, \ldots, x_r = \sigma a_r, x_{r+1} = \cdots = x_{n+1} = 0$ جوابی از (۱) است). برای مشاهدهٔ این امر، خواننده ابتدا باید دو مطلب زیر را تحقیق کند:

(یک) به‌ازای هر $\sigma \in J$، $\{\sigma\tau_1, \sigma\tau_2, \ldots, \sigma\tau_n\} \subset J$، مجموعهٔ نامی از نماینده‌های هم‌مجموعه‌ای H در J است؛

(دو) هرگاه ζ و θ هر دو عنصرهایی از یک هم‌مجموعهٔ H در J باشند، آنگاه (چون $u_i \in H'$)، به‌ازای $i = 1,2, \ldots, n+1$، $\zeta(u_i) = \theta(u_i)$.

از (یک) نتیجه می‌شود که ترتیب محددی مانند $i_1, \ldots, i_{n+1}$ از $1,2, \ldots, n+1$ وجود دارد به‌طوری‌که، به‌ازای هر $k = 1,2, \ldots, n+1$، $\sigma\tau_k$ و τ_{i_k} در یک هم‌مجموعهٔ H در

J قرار می‌گیرند. بنابر (دو)، معادلهٔ k ام (۲) با معادلهٔ i_k ام (۱) یکی است.

لم ۱۰۰۲. *فرض کنیم F یک توسیع میدان K بوده، L و M میدانهایی میانی با* $L \subset M$ *، و H,J زیرگروههایی از گروه گالوای* $Aut_K F$ *با* $H < J$ *باشند.*
(یک) هرگاه L بسته و $[M : L]$ *متناهی باشد، آنگاه M بسته بوده و* $[L' : M'] = [M : L]$ *.*
(دو) هرگاه H بسته و $[J : H]$ *متناهی باشد، آنگاه J بسته بوده و* $[H' : J'] = [J : H]$ *.*
(سه) هرگاه F یک توسیع گالوای با بعد متناهی K باشد، آنگاه تمام میدانهای میانی و تمام زیرگروههای گروه گالوا بسته بوده و $Aut_K F$ *دارای مرتبهٔ* $[F : K]$ *می‌باشد.*

توجه کنید که قسمت (دو) (به‌ازای $H = 1$) ایجاب می‌کند که هر زیرگروه متناهی $\mathbf{Aut}_K F$ بسته باشد.

طرح برهان ۱۰۰۲. (دو) با استفادهٔ متوالی از $J \subset J''$ و $H = H''$ و لمهای ۸۰۲ و ۹۰۲، نتیجه می‌شود که

$$[J : H] \leq [J'' : H] = [J'' : H''] \leq [H' : J'] \leq [J : H];$$

این ایجاب می‌کند که $J = J''$ و $[H' : J'] = [J : H]$. قسمت (یک) به همین نحو ثابت می‌شود.
(سه) هرگاه E یک میدان میانی باشد، آنگاه $[E : K]$ متناهی است (چون $[F : K]$ چنین است). چون F روی K گالواست، K بسته‌بوده و (یک) ایجاب می‌کند که E بسته باشد و $[K' : E'] = [E : K]$. بخصوص، هرگاه $E = F$، آنگاه

$$|\mathrm{Aut}_K F| = [\mathrm{Aut}_K F : 1] = [K' : F'] = [F : K]$$

متناهی است. بنابراین، هر زیرگروه J از $\mathrm{Aut}_K F$ متناهی است. چون 1 بسته است، قسمت (دو) ایجاب می‌کند که J بسته باشد.

قسمت اول قضیهٔ اساسی ۵۰۲ را می‌توان به آسانی از قضیهٔ ۷۰۲ و لم ۱۰۰۲ به دست‌آورد. برای اثبات قسمت (دو) قضیهٔ ۵۰۲، باید تعیین کنیم چه میدانهای میانی نظیر زیرگروههای نرمال گروه گالوا تحت تناظر گالوا هستند. این کار در لم زیر صورت خواهد گرفت.

اگر E یک میدان‌میانی توسیع $K \subset F$ باشد، گوییم E (نسبت به K و F) **پایدار** است اگر هر $\sigma \in \mathrm{Aut}_K F$، E را به توی‌خودبنگارد. هرگاه E پایدار بوده و $\sigma^{-1} \in \mathrm{Aut}_K F$ خودریختی معکوس باشد، آنگاه σ^{-1} نیز E را به توی خود می‌نگارد. این ایجاب می‌کندکه $\sigma | E \in \mathrm{Aut}_K E$ درواقع یک K ــ خودریختی E (یعنی، $\sigma | E$) با معکوس $\sigma^{-1} | E$ باشد. خواهیم دید که، در بعد متناهی، E پایدار است اگر و فقط اگر E روی K گالوا باشد.

لم ۱۱.۲. *فرض کنیم F یک توسیع میدان K باشد.*

(یک) *هرگاه E یک میدان‌میانی پایدار توسیع باشد، آنگاه $E' = Aut_E F$ زیرگروه نرمالی از گروه گالوای $Aut_K F$ است؛*

(دو) *هرگاه H زیرگروه نرمالی از $Aut_K F$ باشد، آنگاه میدان ثابت H' از H یک میدان میانی پایدار توسیع می‌باشد.*

برهان. (یک) هرگاه $u \in E$ و $\sigma \in \mathrm{Aut}_K F$، آنگاه، بنابرپایداری، $\sigma(u) \in E$؛ و درنتیجه، به‌ازای هر $\tau \in E' = \mathrm{Aut}_E F$، $\tau\sigma(u) = \sigma(u)$. بنابراین، به‌ازای هر $\sigma \in \mathrm{Aut}_K F$، $\tau \in E'$، $\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\sigma(u) = u$. درنتیجه، $\sigma^{-1}\tau\sigma \in E'$؛ ولذا، E' در $\mathrm{Aut}_K F$ نرمال است.

(دو) هرگاه $\sigma \in \mathrm{Aut}_K F$ و $\tau \in H$، آنگاه، بنابر نرمالی، $\sigma^{-1}\tau\sigma \in H$. بنابراین، به‌ازای هر $u \in H'$، $\sigma^{-1}\tau\sigma(u) = u$، کـه ایجاب می‌کند که به‌ازای هر $\tau \in H$، $\tau\sigma(u) = \sigma(u)$. لذا، به‌ازای هر $u \in H'$، $\sigma(u) \in H'$، که به معنی پایدار بودن H' است.

در سه لم بعدی روابط بین میدانهای میانی پایدار و توسیعهای گالوا و رابطهٔ هر دو با گروه گالوا به تفصیل به دست می‌آیند.

لم ۱۲.۲. *هرگاه F یک توسیع میدان گالوای K بوده و E یک میدان میانی پایدار توسیع باشد، آنگاه E روی K گالوا می‌باشد.*

برهان. هرگاه $u \in E - K$، آنگاه یک $\sigma \in \mathrm{Aut}_K F$ وجود دارد به‌طوری‌که $\sigma(u) \neq u$، زیرا F

روی K گالواست. اما، بنابر پایداری، $\sigma | E \in \mathrm{Aut}_K E$. بنابراین، طبق تبصرهٔ بعد از تعریف ۴۰۲، E روی K گالواست.

لم ۱۳۰۲. *هرگاه F یک توسیع میدان K بوده و E یک میدان میانی توسیع باشد به‌طوری‌که E روی K جبری و گالوا باشد، آنگاه E (نسبت به F و K) پایدار است.*

تبصره. فرض جبری بودن E لازم است. ر.ک. تمرین ۱۳.

برهان ۱۳۰۲. اگر $u \in E$، فرض می‌کنیم $f \in K[x]$ چندجمله‌ای تحویل‌ناپذیری از u بوده و $u = u_1, u_2, \ldots, u_r$ ریشه‌های متمایز f باشند که در E واقعند. بنابر قضیهٔ III ۷۰۶۰، $r \leq n = \deg f$. هرگاه $\tau \in \mathrm{Aut}_K E$، آنگاه از قضیهٔ ۲۰۲ نتیجه می‌شود که τ صرفاً u_i را جایگشت می‌دهد. این ایجاب می‌کند که ضرایب چندجمله‌ای تکین $g(x) = (x - u_1)(x - u_2)\cdots(x - u_r) \in E[x]$ به‌ازای هر $\tau \in \mathrm{Aut}_K E$ ثابت‌است. چون E روی K گالواست، باید داشته باشیم $g \in K[x]$. اما $u = u_1$ ریشهٔ g است؛ و درنتیجه، $f | g$ (قضیهٔ ۶۰۱ (دو)). چون g تکین بوده و $\deg g \leq \deg f$، باید داشته باشیم $f = g$. درنتیجه، تمام ریشه‌های f متمایز و در E قرار دارند. اما، هرگاه $\sigma \in \mathrm{Aut}_K F$، آنگاه، طبق قضیهٔ ۲۰۲، $\sigma(u)$ ریشه‌ای از f است، که از آنجا $\sigma(u) \in E$. بنابراین، E نسبت به F و K پایدار است.

فرض کنیم E یک میدان میانی توسیع $K \subset F$ باشد. گوییم K ــ خودریختی $\tau \in \mathrm{Aut}_K E$ **توسیع‌پذیر** به F است اگر $\sigma \in \mathrm{Aut}_K F$ ای موجود باشد به‌طوری‌که $\sigma | E = \tau$. به آسانی معلوم می‌شود که K ــ خودریختیهای توسیع‌پذیر زیرگروهی از $\mathrm{Aut}_K E$ تشکیل می‌دهند. به‌یادآورید که اگر E پایدار باشد، $E' = \mathrm{Aut}_E F$ زیرگروه نرمالی از $G = \mathrm{Aut}_K F$ است (لم ۱۱۰۲). درنتیجه، گروه خارج‌قسمتی G/E' تعریف شده است.

لم ۱۴۰۲. *فرض کنیم F یک توسیع میدان K بوده و E یک میدان میانی پایدار توسیع باشد. در این صورت، گروه خارج‌قسمتی $\mathrm{Aut}_K F / \mathrm{Aut}_E F$ با گروه تمام K ــ خودریختیهای E که توسیع‌پذیر به F اند یکریخت است.*

طرح برهان. چون E پایدار است، انتساب $\sigma \mapsto \sigma|E$ یک همریختی گروهها مانند $\mathrm{Aut}_K F \to \mathrm{Aut}_K E$ تعریف می‌کند که نقش آن بوضوح زیرگروه تمام K ـ خودریختیهای E است که به F توسیع پذیرند. توجه کنید که هسته مساوی $\mathrm{Aut}_E F$ است و قضیهٔ اول یکریختی I ۷۰۵۰ را به کار برید.

برهان قضیهٔ ۵۰۲ (قضیهٔ اساسی نظریهٔ گالوا). قضیهٔ ۷۰۲ نشان می‌دهد که تناظر یک به یکی بین میدانهای میانی بستهٔ توسیع و زیرگروههای بستهٔ گروه گالوا وجود دارد. اما دراین حالت، بنابر لم ۱۰۲ (سه)، میدانهای میانی و تمام زیرگروهها بسته‌اند. حکم (یک) قضیه فورا" از لم ۱۰۲ (یک) نتیجه می‌شود.

(دو) F روی E گالواست، زیرا E بسته است (یعنی، $E = E''$). E روی K با بعد متناهی است (زیرا F چنین‌است)؛ و درنتیجه، طبق قضیهٔ ۱۱۰۱، روی K جبری است؛ درنتیجه، هرگاه E روی K گالوا باشد، آنگاه، طبق لم ۱۳۰۲، E پایدار است. بنابر لم ۱۱۰۲ (یک)، $E' = \mathrm{Aut}_E F$ در $\mathrm{Aut}_K F$ نرمال است. به عکس، هرگاه E' در $\mathrm{Aut}_K F$ نرمال باشد، آنگاه E'' یک میدان میانی پایدار است (لم ۱۱۰۲ (دو)). اما $E = E''$، زیراتمام میدانهای میانی بسته بوده؛ و درنتیجه، طبق لم ۱۲۰۲، E روی K گالواست.

فرض کنیم E یک میدان میانی باشد که روی K گالواست (درنتیجه، E' در $\mathrm{Aut}_K F$ نرمال‌است). چون E و E' بسته‌اندو $G' = K$ (F روی K گالواست)، لم ۱۰۲ ایجاب می‌کند که $|G/E'| = [G : E'] = [E'' : G'] = [E : K]$. بنابرلم ۱۴۰۲، $G/E' = \mathrm{Aut}_K F/\mathrm{Aut}_E F$ با زیرگروه $\mathrm{Aut}_K E$ (از مرتبهٔ $[E : K]$) یکریخت‌است. اماقسمت (یک) قضیه نشان می‌دهد که $|\mathrm{Aut}_K E| = [E : K]$ (زیرا E روی K گالواست). این‌ایجاب می‌کند که $G/E' \cong \mathrm{Aut}_K E$.

نظریهٔ جدید گالوا تا حدود زیادی مدیون امیل آرتین است. با آنکه بحث ما مآلا" از آن آرتین (توسط آی. کاپلانسکی) است، روش او با روش داده شده در اینجا از حیث تاکید بر مطالب فرق دارد. دیدگاه آرتین این است که شیء اصلی میدان داده شدهٔ F همراه با گروه (متناهی) G از خودریختیهای F است. سپس زیرمیدان K از F به صورت میدان ثابت G ساخته می‌شود (برهان اینکه زیرمجموعهٔ F که عنصروار توسط G ثابت می‌ماند یک میدان است همان برهان قضیهٔ ۳۰۲ با تغییر مختصر می‌باشد).

قضیهٔ ۱۵۰۲ (آرتین). *فرض کنیم F یک میدان، G گروه خودریختیهای F، و K میدان ثابت G در F باشد. دراین‌صورت، F روی K گالواست. هرگاه G متناهی باشد، آنگاه F یک توسیع گالوا با بعد متناهی K با گروه گالوای G است.*

برهان. در هر حالت، G زیر گروهی از $\mathrm{Aut}_K F$ است. هرگاه $u \in F - K$، آنگاه باید $\sigma \in G$ ای باشد به‌طوری‌که $\sigma(u) \neq u$. بنابراین، میدان ثابت $\mathrm{Aut}_K F$ مساوی K است، که از آنجا F روی K گالواست. هرگاه G متناهی باشد، آنگاه‌لم ۹۰۲ (با $H = 1, J = G$) نشان می‌دهد که $[F : K] = [1' : G'] \leq [G : 1] = |G|$. درنتیجه، F روی K بابعد متناهی است، که ازآنجا، طبق‌لم ۱۰۲ (سه)، $G = G''$. چون طبق فرض $G' = K$ (و درنتیجه، $G'' = K'$)، داریم $\mathrm{Aut}_K F = K' = G'' = G$.

ضمیمه: توابع گویای متقارن

فرض کنیم K یک میدان، $K[x_1, \ldots, x_n]$ دامنهٔ چندجمله‌ای، و $K(x_1, \ldots, x_n)$ میدان توابع گویا باشد (ر.ک. مثال پیش از قضیهٔ ۵۰۱). چون $K(x_1, \ldots, x_n)$ طبق تعریف میدان خارج‌قسمتی $K[x_1, \ldots, x_n]$ است. (تحت انطباق معمولی f با $f/1_K$) داریم $K[x_1, \ldots, x_n] \subset K(x_1, \ldots, x_n)$. فرض کنیم S_n گروه‌متقارن n حرف باشد. تابع گویای $\varphi \in K(x_1, \ldots, x_n)$ را **متقارن** نسبت به $x_1, \ldots, x_n$ روی K گوییم هرگاه به‌ازای هر $\sigma \in S_n$،

$$\varphi(x_1, x_2, \ldots, x_n) = \varphi(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

هرچندجمله‌ای ثابت بداهتاً تابعی متقارن است. هرگاه $n = 4$، آنگاه چندجمله‌ایهای

$$f_1 = x_1 + x_2 + x_3 + x_4,$$

$$f_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$$

$$f_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,$$

و $f_4 = x_1x_2x_3x_4$، همه‌توابعی متقارن‌اند. به‌طور کلی، **توابع متقارن مقدماتی** نسبت به $x_1, \ldots, x_n$ روی K چندجمله‌ایهای زیر تعریف می‌شوند:

$$f_1 = x_1 + x_2 + \cdots + x_n = \sum_{i=1}^{n} x_i;$$

$$f_2 = \sum_{1 \leq i < j \leq n} x_i x_j;$$

$$f_3 = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k;$$

$$f_k = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k};$$

$$\vdots$$

$$f_n = x_1 x_2 \cdots x_n.$$

تحقیق اینکه f_i ها عملاً "متقارن‌اند از این امر نتیجه می‌شود که اینها چیزی جز ضرایب y در چندجمله‌ای $g(y) \in K[x_1, \ldots, x_n][y]$ ، که

$$\begin{aligned} g(y) &= (y - x_1)(y - x_2)(y - x_3) \cdots (y - x_n) \\ &= y^n - f_1 y^{n-1} + f_2 y^{n-2} - \cdots + (-1)^{n-1} f_{n-1} y + (-1)^n f_n \end{aligned}$$

نیستند. هرگاه $\sigma \in S_n$ ، آنگاه انتسابهای $x_i \mapsto x_{\sigma(i)}$ $(i = 1, 2, \ldots, n)$ و

$$f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n) \mapsto f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})/g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

یک K ــ خودریختی از میدان $K(x_1, \ldots, x_n)$ تعریف می‌کنند که با σ نیز نموده می‌شود (تمرین ۱۶). نگاشت $S_n \to \mathrm{Aut}_K K(x_1, \ldots, x_n)$ داده شده با $\sigma \mapsto \sigma$ بوضوح یک تکریختی گروههاست. درنتیجه، S_n را می‌توان زیرگروهی ازگروه گالوای $\mathrm{Aut}_K K(x_1, \ldots, x_n)$ درنظر گرفت. واضح است که میدان ثابت E از S_n در $K(x_1, \ldots, x_n)$ دقیقاً "از توابع متقارن تشکیل‌شده است؛ یعنی، مجموعهٔ تمام توابع متقارن زیرمیدانی از $K(x_1, \ldots, x_n)$ شامل K است. بنابراین، طبق قضیهٔ آرتین ۱۵۰۲، $K(x_1, \ldots, x_n)$ یک توسیع گالوای E با گروه گالوای S_n و بعد $|S_n| = n!$ است.

حکم ۱۶۰۲. *هرگاه G گروهی متناهی باشد، آنگاه یک توسیع میدان گالوا با گروه گالوای یکریخت با G وجوددارد.*

برهان. قضیهٔ کیلی II ۶۰۴۰ می‌گوید که به‌ازای $n = |G|$ ، G با زیرگروهی از S_n (که با G نیز نموده می‌شود) یکریخت است. فرض کنیم K یک میدان و E زیرمیدان توابع گویای متقارن در $K(x_1, \ldots, x_n)$ باشد. بحث پیش ازقضیه‌نشان می‌دهد که $K(x_1, \ldots, x_n)$ یک توسیع گالوای E با گروه گالوای S_n است. برهان قضیهٔ اساسی ۵۰۲ نشان می‌دهدکه $K(x_1, \ldots, x_n)$ یک توسیع گالوای میدان ثابت E_1 از G است به‌طوری‌که $\mathrm{Aut}_{E_1} K(x_1, \ldots, x_n) = G$.

بقیهٔ این ضمیمه (که فقط در ضمیمهٔ بخش ۹ به کار خواهد رفت) اختصاص به اثبات دو قضیهٔ کلاسیک در باب توابع متقارن دارد. در سراسر این بحث، n عدد صحیح مثبتی است، K میدانی دلخواه است، E زیرمیدان توابع گویای متقارن در $K(x_1, \ldots, x_n)$ است، و $f_1, \ldots, f_n \in E$ توابع متقارن مقدماتی نسبت به متغیرهای $x_1, \ldots, x_n$ روی K می‌باشند. زنجیری از میدانها خواهیم داشت:

$$K \subset K(f_1, \ldots, f_n) \subset E \subset K(x_1, \ldots, x_n).$$

در قضیهٔ ۱۸۰۲ نشان خواهیم داد که $E = K(f_1, \ldots, f_n)$.

هرگاه $u_1, \ldots, u_r \in K(x_1, \ldots, x_n)$، آنگاه هر عنصر $K(u_1, \ldots, u_r)$ به شکل $g(u_1, \ldots, u_r)/h(u_1, \ldots, u_r)$ است که در آن، طبق قضیهٔ ۳۰۱، $g, h \in K[x_1, \ldots, x_r]$. درنتیجه، یک عنصر $K(u_1, \ldots, u_r)$ [$K[u_1, \ldots, u_r]$] معمولاً" تابعی گویا [چندجمله‌ای] از $u_1, \ldots, u_r$ روی K نام دارد. لذا، عبارت $E = K(f_1, \ldots, f_n)$ را می‌توان چنین بیان کرد: هر تابع متقارن گویا درواقع تابعی گویا از توابع متقارن مقدماتی $f_1, \ldots, f_n$ روی K است. برای اثبات $E = K(f_1, \ldots, f_n)$ به لم زیر نیاز خواهیم داشت.

لم ۱۷۰۲. *فرض کنیم K یک میدان، $f_1, \ldots, f_n$ توابع متقارن مقدماتی از $x_1, \ldots, x_n$ روی K، و k عددی صحیح با $1 \leq k \leq n-1$ باشد. هرگاه $h_1, \ldots, h_k \in K[x_1, \ldots, x_n]$ توابع متقارن مقدماتی از $x_1, \ldots, x_k$ باشند، آنگاه هر h_j را می‌توان به صورت یک چندجمله‌ای روی K از $f_1, f_2, \ldots, f_n$ و $x_{k+1}, x_{k+2}, \ldots, x_n$ نوشت.*

طرح برهان. قضیه وقتی $k = n-1$ درست است، زیرا در آن صورت $h_1 = f_1 - x_n$ و $h_j = f_j - h_{j-1}x_n$ $(2 \leq j \leq n)$. برهان را با استقرا بر k به ترتیب عکس کامل می‌کنیم: فرض کنیم قضیه وقتی $k = r+1 \leq n-1$ درست باشد. همچنین، $g_1, \ldots, g_{r+1}$ توابع متقارن مقدماتی از $x_1, \ldots, x_{r+1}$ و $h_1, \ldots, h_r$ توابع متقارن مقدماتی از $x_1, \ldots, x_r$ باشند. چون $h_1 = g_1 - x_{r+1}$ و $h_j = g_j - h_{j-1}x_{r+1}$ $(2 \leq j \leq r)$، نتیجه می‌شود که قضیه به‌ازای $k = r$ نیز درست است.

قضیهٔ ۱۸۰۲. *هرگاه K میدان، E زیرمیدان تمام توابع گویای مقدماتی در $K(x_1, \ldots, x_n)$، و $f_1, \ldots, f_n$ توابع متقارن مقدماتی باشند، آنگاه $E = K(f_1, \ldots, f_n)$.*

طرح برهان. چون $[K(x_1,\dots,x_n):E]=n!$ و $K(f_1,\dots,f_n)\subset E\subset K(x_1,\dots,x_n)$، طبق قضیهٔ ۲۰۱ کافی است نشان دهیم که $[K(x_1,\dots,x_n):K(f_1,\dots,f_n)]\le n!$. فرض کنیم $F=K(f_1,\dots,f_n)$ و زنجیر زیر از میدانها را درنظر می‌گیریم:

$$F\subset F(x_n)\subset F(x_{n-1},x_n)\subset\cdots\subset F(x_2,\dots,x_n)\subset F(x_1,\dots,x_n)=K(x_1,\dots,x_n).$$

چون $F(x_k,x_{k+1},\dots,x_n)=F(x_{k+1},\dots,x_n)(x_k)$، طبق قضایای ۲۰۱ و ۶۰۱ کافی است نشان دهیم که x_n روی F جبری از درجهٔ نابیشتر از n است و، به‌ازای هر $k<n$، x_k روی $F(x_{k+1},\dots,x_n)$ جبری از درجهٔ نابیشتر از k می‌باشد. برای این کار، فرض کنیم $g_n(y)\in F[y]$ چندجمله‌ای

$$g_n(y)=(y-x_1)(y-x_2)\cdots(y-x_n)=y^n-f_1y^{n-1}+\cdots+(-1)^nf_n$$

باشد. ازآنجا که تابع $g_n\in F[y]$ ازدرجهٔ n بوده و x_n ریشه‌ای از g_n است، بنابر قضیهٔ ۶۰۱، x_n جبری از درجهٔ حداکثر n روی $F=K(f_1,\dots,f_n)$ می‌باشد، حال، به‌ازای هر k $(1\le k<n)$، چندجمله‌ای تکین زیر را تعریف می‌کنیم:

$$g_k(y)=g_n(y)/(y-x_{k+1})\cdots(y-x_n)=(y-x_1)(y-x_2)\cdots(y-x_k).$$

واضح است‌که هر $g_k(y)$ از درجهٔ k است، x_k ریشه‌ای از $g_k(y)$ است، و ضرایب $g_k(y)$ دقیقاً" توابع متقارن مقدماتی از $x_1,\dots,x_k$ اند. بنابر لم ۱۷۰۲، هر $g_k(y)$ در $F(x_{k+1},\dots,x_n)[y]$ قرار دارد؛ درنتیجه، x_k روی $F(x_{k+1},\dots,x_n)$ جبری از درجهٔ حداکثر k می‌باشد.

حال مشابه قضیه ۱۸۰۲ را برای توابع **چندجمله‌ای** متقارن ثابت می‌کنیم؛ یعنی، ثابت می‌کنیم هرچندجمله‌ای متقارن از $x_1,\dots,x_n$ روی K عملاً" یک چندجمله‌ای از توابع متقارن مقدماتی $f_1,\dots,f_n$ روی K است. به عبارت دیگر، هر چندجمله‌ای متقارن از $K[x_1,\dots,x_n]$ در $K[f_1,\dots,f_n]$ قرار دارد. ابتدا به لم زیر نیاز داریم.

لم ۱۹۰۲. *فرض کنیم K میدان و E زیرمیدان تمام توابع گویای متقارن در $K(x_1,\dots,x_n)$ باشد. دراین صورت، مجموعهٔ $X=\{x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\mid 0\le i_k<k,\ k$ به‌ازای هر $\}$ پایه‌ای از $K(x_1,\dots,x_n)$ روی E است.*

طرح برهان. چون $[K(x_1,\dots,x_n):E]=n!$ و $|X|=n!$، کافی است نشان دهیم که X،

$K(x_1,\ldots,x_n)$ را می‌پیماید (ر.ک. قضیهٔ IV ۵۰۲۰) . زنجیر

$$E \subset E(x_n) \subset E(x_{n-1},x_n) \subset \cdots \subset E(x_1,\ldots,x_n) = K(x_1,\ldots,x_n)$$

از میدانها را درنظر می‌گیریم . چون (بنابر برهان قضیهٔ ۱۸۰۲) x_n روی E جبری از درجهٔ نابیشتر از n است، مجموعهٔ $\{x_n^j \mid 0 \le j < n\}$ ، $E(x_n)$ را روی E می‌پیماید (قضیهٔ ۶۰۱) . چون $E(x_{n-1},x_n) = E(x_n)(x_{n-1})$ ، و x_{n-1} روی $E(x_n)$ جبری از درجهٔ نابیشتر از $n-1$ است، مجموعهٔ $\{x_{n-1}^i \mid 0 \le i < n-1\}$ ، $E(x_{n-1},x_n)$ را روی $E(x_n)$ می‌پیماید . استدلال آمده در بند دوم برهان قضیهٔ IV ۶۰۲۰ نشان می‌دهد که مجموعهٔ $\{x_{n-1}^i x_n^j \mid 0 \le i < n-1; 0 \le j < n\}$ ، $E(x_{n-1},x_n)$ را روی E می‌پیماید . این اولین گام در یک برهان استقرایی است، که با استدلالهای مشابهی کامل می‌شود .

حکم ۲۰۰۲ . *فرض کنیم* K *میدان و* $f_1,\ldots,f_n$ *توابع متقارن مقدماتی در* $K(x_1,\ldots,x_n)$ *باشند .*

(یک) *هر چندجمله‌ای در* $K[x_1,\ldots,x_n]$ *را می‌توان به‌طور منحصربه‌فرد به صورت ترکیبی خطی از* $n!$ *عنصر* $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ ($0 \le i_k < k$ *به‌ازای هر* k) *با ضرایب در* $K[f_1,\ldots,f_n]$ *نوشت :*

(دو) *هر چندجمله‌ای متقارن در* $K[x_1,\ldots,x_n]$ *در* $K[f_1,\ldots,f_n]$ *قرار دارد .*

برهان . فرض کنیم $g_k(y)$ $(k = 1,\ldots,n)$ همانند در برهان قضیهٔ ۱۸۰۲ باشند . همانطورکه‌گفتیم ،ضرایب $g_k(y)$ چندجمله‌ایهایی (روی K) از $f_1,\ldots,f_n$ و $x_{k+1},\ldots,x_n$ هستند . چون g_k تکین از درجهٔ k است و $g_k(x_k) = 0$ ، x_k^k را می‌توان به صورت یک چندجمله‌ای روی K از $f_1,\ldots,f_n$ ، $x_{k+1},\ldots,x_n$ ، و x_k^i $(i \le k-1)$ بیان کرد . اگر قدم بـه قدم پیش رفته با $k = 1$ شروع کنیم و عبارت مربوط به x_k^k را در چندجمله‌ای $h \in K[x_1,\ldots,x_n]$ قرار دهیم ، نتیجه یک چندجمله‌ای از $f_1,\ldots,f_n, x_1,\ldots,x_n$ خواهد بود که بالاترین نمای هر x_k مساوی $k-1$ است . به عبارت دیگر ، h ترکیبی خطی از $n!$ عنصر $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ ($i_k < k$ به‌ازای هر k) است با ضرایب در $K[f_1,\ldots,f_n]$. به علاوه ، این چندجمله‌ایهای ضرایب به‌طور منحصر به فرد معین می‌شوند ، زیرا ، بنابر لم ۱۹۰۲ ،

$\{x_1^{i_1}\cdots x_n^{i_n} \mid 0 \le i_k < k$ ، k به‌ازای هر

روی $E = K(f_1, \ldots, f_n)$ مستقل خطی است. این قسمت (یک) را ثابت کرده و نیز ایجاب می‌کند که هرگاه چندجمله‌ای $h \in K[x_1, \ldots, x_n]$ ترکیبی خطی از $x_1^{i_1} \cdots x_n^{i_n}$ $(i_k < k)$ با ضرایب در $K(f_1, \ldots, f_n)$ باشد، آنگاه ضرایب عملاً "چندجمله‌ایهایی در $K[f_1, \ldots, f_n]$ می‌باشند. بخصوص، هرگاه h یک‌چندجمله‌ای متقارن باشد (یعنی، $h \in E = K(f_1, \ldots, f_n)$)، آنگاه $h = hx_1^0x_2^0 \cdots x_n^0$ لزوماً "در $K[f_1, \ldots, f_n]$ قرار دارد. این قسمت (دو) را ثابت می‌کند.

تمرینات

تذکر. F همواره یک توسیع میدان از میدان K و E یک میدان میانی توسیع است مگر آنکه خلافش گفته شود.

۱. (آ) هرگاه F میدان و $\sigma : F \to F$ یک همریختی (حلقه‌ها) باشد، آنگاه $\sigma = 0$ یا σ یک تکریختی است. هرگاه $\sigma \neq 0$، آنگاه $\sigma(1_F) = 1_F$.

(ب) مجموعهٔ $\mathrm{Aut}\, F$ مرکب‌از تمام خودریختیهای میدانهای $F \to F$ یک گروه تحت عمل ترکیب توابع تشکیل می‌دهد.

(پ) $\mathrm{Aut}_K F$، یعنی مجموعهٔ تمام K ــ خودریختیهای F، زیرگروهی از $\mathrm{Aut}\, F$ است.

۲. $\mathrm{Aut}_{\mathbf{Q}}\mathbf{R}$ گروه همانی است. [**راهنمایی.** چون هر عنصر مثبت $\mathbf{R}$ مربع است، نتیجه می‌شود که یک خودریختی $\mathbf{R}$ مثبت را به مثبت برده، و درنتیجه، ترتیب‌را در $\mathbf{R}$ حفظ می‌کند. یک عدد حقیقی داده شده را بین اعداد گویای مناسبی محصور کنید.]

۳. هرگاه $0 \leq d \in \mathbf{Q}$، آنگاه $\mathrm{Aut}_{\mathbf{Q}}\mathbf{Q}(\sqrt{d})$ همانی یا با Z_2 یکریخت است.

۴. گروه گالوای $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ روی $\mathbf{Q}$ چیست؟

۵. (آ) هرگاه $0 \leq d \in \mathbf{Q}$، آنگاه $\mathbf{Q}(\sqrt{d})$ روی $\mathbf{Q}$ گالوا است.

(ب) $\mathbf{C}$ روی $\mathbf{R}$ گالوا است.

۶. فرض کنید $f/g \in K(x)$، که در آن $f/g \notin K$ و f, g در $K[x]$ نسبت به هم اولند، و توسیع K به وسیلهٔ $K(x)$ را درنظر بگیرید.

(آ) x روی $K(f/g)$ جبری است و $[K(x) : K(f/g)] = \max(\deg f, \deg g)$.

[**راهنمایی.** x ریشه‌ای از چندجمله‌ای ناصفر $\varphi(y) = (f/g)g(y) - f(y) \in K(f/g)[y]$

است؛ نشان‌دهید φ از درجهٔ $\max(\deg f,\deg g)$ است. نشان‌دهید φ تحویل‌ناپذیر است، به صورت زیر.

چون f/g روی K متعالی است (چرا؟)، می‌توان برای راحتی $K(f/g)$ را با $K(z)$ (z مجهول) عوض کرده و $\varphi = zg(y) - f(y) \in K(z)[y]$ را درنظرگرفت. بنابر لم III ۱۳.۶، φ در $K(z)[y]$ تحویل‌ناپذیر است مشروط بر اینکه در $K[z][y]$ تحویل‌ناپذیر باشد. صحت شرط دوم از این ناشی می‌شود که φ نسبت به z خطی بوده و f,g نسبت به هم اولند.]

(ب) هرگاه $E \neq K$ یک میدان میانی باشد، آنگاه $[K(x) : E]$ متناهی است.

(پ) انتساب $x \mapsto f/g$ همریختی $\sigma : K(x) \to K(x)$ را القا می‌کند به‌طوری که $\varphi(x)/\psi(x) \mapsto \varphi(f/g)/\psi(f/g)$. σ یک K ـ خودریختی $K(x)$ است اگر و فقط اگر $\max(\deg f,\deg g) = 1$.

(ت) $\mathrm{Aut}_K K(x)$ از تمام خودریختیهایی تشکیل شده است که (همانند در (پ)) با انتساب

$$x \mapsto (ax + b)/(cx + d),$$

که در آن $a,b,c,d \in K$ و $ad - bc \neq 0$، القا می‌شوند.

۷. فرض کنید G زیرمجموعه‌ای از $\mathrm{Aut}_K K(x)$ مرکب از سه خودریختی باشد که (همانند در ۶ (پ)) به وسیلهٔ $x \mapsto x, x \mapsto 1_K/(1_K - x), x \mapsto (x - 1_K)/x$ القا می‌شوند. در این صورت، G زیرگروهی از $\mathrm{Aut}_K K(x)$ می‌باشد. میدان ثابت G را تعیین کنید.

۸. فرض کنید $\mathrm{char}\, K = 0$ و G زیرگروه $\mathrm{Aut}_K K(x)$ باشد که با خودریختی تولید شده به وسیلهٔ $x \mapsto x + 1_K$ القا می‌شود. در این صورت، G یک گروه دوری نامتناهی است. میدان ثابت E از G را تعیین کنید. $[K(x) : E]$ چیست؟

۹. (آ) هرگاه K یک میدان نامتناهی باشد، آنگاه $K(x)$ روی K گالواست.

[**راهنمایی.** هرگاه $K(x)$ روی K گالوا نباشد، آنگاه، بنابر تمرین ۶ (ب)، $K(x)$ روی میدان ثابت E از $\mathrm{Aut}_K K(x)$ با بعد متناهی است. اما، طبق تمرین ۶ (ت)، $\mathrm{Aut}_E K(x) = \mathrm{Aut}_K K(x)$، که با لم ۸.۲ در تضاد است.]

(ب) هرگاه K متناهی باشد، آنگاه $K(x)$ روی K گالوا **نیست**.

[**راهنمایی.** هرگاه $K(x)$ روی K گالوا می‌بود، $\mathrm{Aut}_K K(x)$ طبق لم ۹.۲ نامتناهی می‌شد. اما، طبق تمرین ۶ (ت)، $\mathrm{Aut}_K K(x)$ متناهی است.]

۱۰ . هرگاه K میدانی نامتناهی باشد ، آنگاه تنها زیرگروههای بستهٔ $\mathrm{Aut}_K K(x)$ خود و زیرگروههای متناهی آن می‌باشند . [**راهنمایی** . ر.ک. تمرینهای ۶ (ب) و ۹ .]

۱۱ . در توسیع $\mathbf{Q}$ به وسیلهٔ $\mathbf{Q}(x)$ ، میدان میانی $\mathbf{Q}(x^2)$ بسته است ولی $\mathbf{Q}(x^3)$ چنین نیست .

۱۲ . هرگاه E یک میدان میانی از توسیع باشد به‌طوری‌که E روی K گالوا است ، F روی E گالوا باشد ، و هر $\sigma \in \mathrm{Aut}_K E$ توسیع پذیر به F باشد . آنگاه F روی K گالوا می‌باشد .

۱۳ . در توسیع میدان نامتناهی K به وسیلهٔ $K(x,y)$ ، میدان میانی $K(x)$ روی K گالوا است ولی (نسبت به $K(x,y)$ و K) پایدار نیست . [ر.ک. تمرین ۹ ؛ این نتیجه را با لم ۱۳.۲ مقایسه کنید .]

۱۴ . فرض کنید F یک توسیع گالوای با بعد متناهی K بوده و L و M دو میدان میانی باشند .

(آ) $\mathrm{Aut}_{LM} F = \mathrm{Aut}_L F \cap \mathrm{Aut}_M F$.

(ب) $\mathrm{Aut}_{L\cap M} F = \mathrm{Aut}_L F \vee \mathrm{Aut}_M F$.

(پ) اگر $\mathrm{Aut}_L F \cap \mathrm{Aut}_M F = 1$ ، چه نتیجه‌ای می‌توان گرفت ؟

۱۵ . هرگاه F یک‌توسیع گالوای با بعد متناهی K و E یک میدان میانی باشد ، آنگاه کوچکترین میدان منحصربه فرد L وجود دارد به‌طوری‌که $E \subset L \subset F$ و L روی K گالوا است . به علاوه ،

$$\mathrm{Aut}_L F = \bigcap_{\sigma} \sigma(\mathrm{Aut}_E F)\sigma^{-1},$$

که در آن σ روی $\mathrm{Aut}_K F$ تغییر می‌کند .

۱۶ . هرگاه $\sigma \in S_n$ ، آنگاه نگاشت $K(x_1, \ldots, x_n) \to K(x_1, \ldots, x_n)$ داده شده با

$$\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \mapsto \frac{f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}$$

یک K ــ خودریختی $K(x_1, \ldots, x_n)$ می‌باشد .

۳ میدانهای تجزیه‌گر ، بست جبری و نرمالی

حال به مسئلهٔ تشخیص و/یا ساختن توسیعهای گالوا رومی‌آوریم . میدانهای تجزیه‌گر ، که موضوع اصلی ایــن بخش‌اند ، ما را به انجام این کار قادر می‌سازند . ابتدا خواص اساسی میدانهای تجزیه‌گرو بستهای جبری (حالت خاصی از میدانهای تجزیه‌گر) را عرضه می‌کنیم.

سپس توسیعهای گالوای جبری را با اصطلاحاتی توصیف می‌کنیم که در آنها گروه گالوا صریحا "ذکر نشده است،(قضیهٔ ۱۱.۳) ، و قضیهٔ اساسی‌را به حالت جبری با بعد نامتناهی تعمیم می‌دهیم (قضیهٔ ۱۲.۳) . بالاخره ، نرمالی و ویژگیهای دیگر میدانهای تجزیه‌گر را مطرح خواهیم کرد . قضیهٔ اساسی جبر (هر معادلهٔ چندجمله‌ای روی اعداد مختلط جواب دارد) در ضمیمه ثابت شده است .

فرض کنیم F میدان و $f \in F[x]$ یک‌چندجمله‌ای‌از درجهٔ **مثبت** باشد . گوییم f روی F **تجزیه می‌شود** (یا در $F[x]$ تجزیه می‌شود) اگر f را بتوان به صورت حاصلضربی از عوامل خطی در $F[x]$ نوشت؛ یعنی ، $f = u_0(x - u_1)(x - u_2)\cdots(x - u_n)$ ، که در آن $u_i \in F$.

تعریف ۱.۳ . فرض کنیم K میدان و $f \in K[x]$ یک چندجمله‌ای از درجهٔ مثبت باشد . گوییم توسیع میدان F از K یک ***میدان تجزیه‌گر چند جمله‌ای*** f **روی** K است اگر f در $F[x]$ تجزیه شده و $F = K(u_1, \ldots, u_n)$ ، که‌درآن $u_1, \ldots, u_n$ ریشه‌های f در F می‌باشند .

فرض کنیم S مجموعه‌ای از چندجمله‌ایها از درجهٔ مثبت در $K[x]$ باشد . گوییم توسیع میدان F از K یک ***میدان تجزیه‌گر مجموعهٔ*** S ***از چندجمله‌ایها روی*** K است اگر هر چندجمله‌ای‌در S در $F[x]$ تجزیه‌شده‌و F روی K با ریشه‌های تمام چندجمله‌ایها در S تولید گردد .

چند مثال . تنها ریشه‌های $x^2 - 2$ روی $\mathbf{Q}$ عبارتند از $\sqrt{2}$ و $-\sqrt{2}$. بنابراین ، $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\sqrt{2}, -\sqrt{2})$ یک میدان تجزیه‌گر $x^2 - 2$ روی $\mathbf{Q}$ است . به‌همین ترتیب ، $\mathbf{C}$ یک میدان تجزیه‌گر $x^2 + 1$ روی $\mathbf{R}$ است . اما ، اگر u ریشه‌ای‌ازچندجمله‌ای‌تحویل‌ناپذیر $f \in K[x]$ باشد ، $K(u)$ لزوما "یک میدان تجزیه‌گر f نیست . مثلا" ، هرگاه u ریشهٔ سوم حقیقی 2 باشد (ریشه‌های دیگر مختلط‌اند) ، آنگاه $\mathbf{Q}(u) \subset \mathbf{R}$ ؛ درنتیجه ، $\mathbf{Q}(u)$ میدان تجزیه‌گر $x^3 - 2$ روی $\mathbf{Q}$ نیست .

چند تبصره . هرگاه F یک میدان تجزیه‌گر S روی K باشد ، آنگاه $F = K(X)$ که در آن X مجموعهٔ تمام ریشه‌های چندجمله‌ایها در زیرمجموعهٔ S از $K[x]$ است . قضیهٔ ۱۲.۱ فورا "ایجاب می‌کندکه F روی K جبری است (و با بعد متناهی اگر S ، و درنتیجه

X ، مجموعه‌ای متناهی باشد) . توجه کنید که هرگاه S متناهی باشد، مثلا " $S = \{f_1, f_2, \ldots, f_n\}$ ، آنگاه یک میدان تجزیه‌گر S یا یک میدان تجزیه‌گر چندجمله‌ای $f = f_1 f_2 \cdots f_n$ یکی است (تمرین ۱) . ازاین مطلب درآینده مکرر بدون ذکر صریح استفاده خواهد شد . لذا ، میدان تجزیه‌گر مجموعهٔ S از چندجمله‌ایها وقتی مورد توجه قرار می‌گیرد که S از یک چندجمله‌ای تشکیل شده باشد یا نامتناهی باشد . خواهیم دید که هرتوسیع گالوای جبری [با بعد متناهی] عملا " نوع خاصی میدان تجزیه‌گر از یک مجموعهٔ [متناهی] از چندجمله‌ایهاست .

سئوال روشنی که اینک پاسخ می‌خواهد این است که آیا هر مجموعه از چندجمله‌ایها میدان تجزیه‌گر دارد . در حالت یک چندجمله‌ای (یا ، معادلا " ، مجموعه‌ای متناهی از چندجمله‌ایها) ، جواب نسبتا " آسان است .

قضیهٔ ۲۰۳ . هرگاه K میدان بوده و $f \in K[x]$ از درجهٔ $n \geq 1$ باشد ، آنگاه یک میدان تجزیه‌گر مانند F از f وجود دارد که $[F : K] \leq n!$.

طرح برهان . به استقرا بر $n = \deg f$ عمل می‌کنیم . هرگاه $n = 1$ یا f روی K تجزیه شود ، آنگاه $F = K$ یک میدان تجزیه‌گراست . اگر $n > 1$ و f روی K تجزیه نشود ، $g \in K[x]$ را یک عامل تحویل‌ناپذیر f از درجهٔ بزرگتر از یک می‌انگاریم . بنابر قضیهٔ ۱۰.۱ ، یک توسیع میدان ساده مانند $K(u)$ از K هست به‌طوری‌که u ریشه‌ای از g بوده و $[K(u) : K] = \deg g > 1$. در این صورت ، طبق قضیهٔ III ۶.۶۰ ، $f = (x - u)h$ ، که در آن $h \in K(u)[x]$ از درجهٔ $n - 1$ است . بنابراستقرا ، یک میدان تجزیه‌گر F از h روی $K(u)$ و با بعد حداکثر $(n-1)!$ وجود دارد . نشان دهید که F یک میدان تجزیه‌گر f روی K (تمرین ۳) با بعد $\leq n!$ می‌باشد . $[F : K] = [F : K(u)][K(u) : K] \leq (n-1)!\,(\deg g)$

اثبات وجود میدان تجزیه‌گر یک مجموعهٔ نامتناهی از چندجمله‌ایها خیلی مشکلتر است . ما ، بامعرفی حالت خاصی از این نوع میدان تجزیه‌گر (قضیهٔ ۴.۳) که خود اهمیت زیادی دارد ، به‌طور غیرمستقیم به برهان نزدیک می‌شویم .

تذکر . خواننده‌ای که فقط به میدانهای تجزیه‌گر یک چندجمله‌ای (یعنی ، میدانهای

تجزیه‌گر بابعدمتناهی) علاقه‌منداست می‌تواند مطالب را تا قضیهٔ ۸۰۳ حذف کند. باید قضیهٔ ۱۲۰۳ حذف شده و قضایای ۸۰۳ تا ۱۶۰۳ در بعد متناهی خوانده شوند. اثبات هریک از این نتایج یا به دو حالت تقسیم می‌شوند (ابعاد متناهی و نامتناهی) یا مستقیما" در هر دو حالت به کار می‌روند. تنها استثنا در اثبات (یک) $\Rightarrow$ (دو) درقضیهٔ ۱۴۰۳ است؛ برهانی دیگر در تمرین ۲۵ پیشنهاد شده است.

قضیهٔ ۳۰۳. *شرایط زیر بر میدان F باهم معادلند:*

(یک) *هر چندجمله‌ای غیرثابت* $f \in F[x]$ *ریشه‌ای در F دارد؛*

(دو) *هر چندجمله‌ای غیرثابت* $f \in F[x]$ *روی F تجزیه می‌شود؛*

(سه) *هر چندجمله‌ای تحویل‌ناپذیر در* $F[x]$ *از درجهٔ یک است؛*

(چهار) *هیچ توسیع میدان جبری از F (به جز خود F) وجود ندارد؛*

(پنج) *یک زیرمیدان مانند K از F وجود دارد به‌طوری‌که F روی K جبری بوده و هر چندجمله‌ای در* $K[x]$ *در* $F[x]$ *تجزیه می‌شود.*

برهان. تمرین. ر.ک. بخش III ۶۰ و قضایای ۶۰۱، ۱۰۰۱، ۱۲۰۱، و ۱۳۰۱.

گوییم هرمیدان صادق درشرایط معادل قضیهٔ ۳۰۳ *به‌طور جبری بسته است*. مثلا"، نشان خواهیم داد که میدان اعداد مختلط **C** به‌طور جبری بسته است (قضیهٔ ۱۹۰۳).

قضیهٔ ۴۰۳. *هرگاه F توسیع میدانی از K باشد، آنگاه شرایط زیر باهم معادلند:*

(یک) *F روی K جبری و F به‌طور جبری بسته است؛*

(دو) *F یک میدان تجزیه‌گر روی K از مجموعهٔ تمام چندجمله‌ایهای [تحویل‌ناپذیر] در* $K[x]$ *است.*

برهان. تمرین؛ همچنین، ر.ک. تمرینات ۹ و ۱۰.

توسیع میدان F از میدان K که در شرایط معادل قضیهٔ ۴۰۳ صدق کند یک *بست جبری* K نام دارد. مثلا"، $\mathbf{C} = \mathbf{R}(i)$ بست‌جبری **R** است. واضح است که هرگاه F بست

جبری K بوده و S مجموعه‌ای از چندجمله‌ایها در $K[x]$ باشد، آنگاه، بنابر قضایای ۳۰۳ و ۴۰۳، زیرمیدان E از F که به وسیلهٔ K و تمام ریشه‌های چندجمله‌ایهای در S تولید می‌شود یک میدان تجزیه‌گر S روی K می‌باشد. لذا، وجود میدانهای تجزیه‌گر دلخواه روی میدان K معادل است با وجود یک بست جبری از K.

مشکل عمده در اثبات اینکه هر میدان K یک بست جبری دارد بیشتر نظریهٔ مجموعه‌ای است تا جبری. ایدهٔ اصلی اعمال لم زرن بر **مجموعه‌ای** از توسیعهای میدان جبری از K است که مناسب اختیار شده باشد[1] برای این کار، به لم زیر نیاز داریم.

لم ۵۰۳. *هرگاه F یک توسیع میدان جبری K باشد، آنگاه $|F| \leq \aleph_0|K|$.*

طرح برهان. فرض کنیم T مجموعهٔ چندجمله‌ایهای تکین از درجهٔ مثبت در $K[x]$ باشد. ابتدا نشان می‌دهیم $|T| = \aleph_0|K|$. به‌ازای هر $n \in \mathbf{N}^*$، فرض کنیم T_n مجموعهٔ تمام چندجمله‌ایها در T از درجهٔ n باشد. پس $|T_n| = |K^n|$، که در آن $K^n = K \times K \times \cdots K$ (n عامل)، زیرا هر چندجمله‌ای $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in T_n$ کاملا" با n ضریب خود $a_0, a_1, \ldots, a_{n-1} \in K$ معین می‌شود. به‌ازای هر $n \in \mathbf{N}^*$، فرض می‌کنیم $f_n : T_n \to K^n$ یک بیژکسیون باشد. چون مجموعه‌های T_n [K^n] دو به دو از هم جدایند، نگاشت $f : T = \bigcup_{n \in \mathbf{N}^*} T_n \to \bigcup_{n \in \mathbf{N}^*} K^n$، داده شده با $f(u) = f_n(u)$ به‌ازای $u \in T_n$، یک بیژکسیون تعریف شده است. بنابراین، طبق آشنایی، قضیهٔ ۱۲۰۸ (دو)، $|T| = |\bigcup_{n \in \mathbf{N}^*} K^n| = \aleph_0|K|$.

حال نشان می‌دهیم $|F| \leq |T|$، که برهان را تمام خواهد کرد. به‌ازای هر $f \in T$ تحویل‌ناپذیر، ترتیبی به ریشه‌های متمایز f در F می‌دهیم. نگاشت $F \to T \times \mathbf{N}^*$ را به صورت زیر تعریف می‌کنیم. هرگاه $a \in F$، آنگاه، طبق فرض، a روی K جبری است، و یک چندجمله‌ای تکین تحویل‌ناپذیر منحصر به‌فرد مانند $f \in T$ با خاصیت $f(a) = 0$ وجود دارد (قضیهٔ ۶۰۱). به $a \in F$ جفت $(f, i) \in T \times \mathbf{N}^*$ را نسبت می‌دهیم که a ریشهٔ i م

---

۱. هرکس با پارادکسهای نظریهٔ مجموعه‌ها (آشنایی، بخش ۲) آشنا باشد ممکن است بگوید که ردهٔ *تمام* توسیعهای میدان جبری لزوما" مجموعه نیست؛ و لذا، نمی‌تواند در این گونه استدلال به‌کار رود.

f درترتیب‌ریشه‌های f در F است که قبلا" اختیار شده است. تحقیق کنید که این نگاشت $F \to T \times \mathbf{N}^*$ تعریف شده و انژکتیو است. چون T نامتناهی است، طبق قضیهٔ ۱۱۰۸، آشنایی، $|F| \leq |T \times \mathbf{N}^*| = |T||\mathbf{N}^*| = |T|\aleph_0 = |T|$.

قضیهٔ ۶۰۳. هر میدان K دارای بست‌جبری است. هردو بست جبری K، K ـ یکریخت می‌باشند.

طرح برهان. مجموعهٔ S را طوری می‌گیریم که $\aleph_0|K| < |S|$ (این همواره به وسیلهٔ قضیهٔ ۵۰۸ آشنایی میسر است). چون $|K| \leq \aleph_0|K|$ (آشنایی، قضیهٔ ۱۱۰۸)، طبق تعریف ۴۰۸ آشنایی، یک نگاشت انژکتیو مانند $\theta : K \to S$ وجود دارد. درنتیجه، می‌توان فرض کرد $K \subset S$ (در غیر این صورت، S را با اجتماع $S - \operatorname{Im}\theta$ و K عوض می‌کنیم).

فرض کنیم $\mathcal{S}$ ردهٔ تمام میدانهای E باشدبه‌طوری‌که E زیرمجموعه‌ای از S بوده‌و E یک توسیع میدان جبری از K است. این E کاملا" با زیرمجموعهٔ E از S و اعمال دوتایی جمع و ضرب در E معین می‌شود. اما جمع ضرب] تابعی مانند $\varphi : E \times E \to E$ [یا $\psi : E \times E \to E$] است. از اینرو، φ [یا ψ] را می‌توان با نمودارش، که زیرمجموعه‌ای از $S \times S \times S$ است، یکی کرد (ر.ک. آشنایی، بخش ۴). درنتیجه، یک نگاشت انژکتیو مانند τ از $\mathcal{S}$ به توی مجموعهٔ P مرکب از تمام زیرمجموعه‌های مجموعهٔ $S \times (S \times S \times S) \times (S \times S \times S)$، که با $E \mapsto (E, \varphi, \psi)$ داده می‌شود، وجود دارد. اما $\operatorname{Im}\tau$ عملا" مجموعه است، زیرا $\operatorname{Im}\tau$ زیر رده‌ای از مجموعهٔ P است. چون $\mathcal{S}$ نقش $\operatorname{Im}\tau$ تحت تابع $\tau^{-1} : \operatorname{Im}\tau \to \mathcal{S}$ است، اصول موضوع نظریهٔ مجموعه‌ها مجموعه بودن $\mathcal{S}$ را تضمین خواهد کرد.

توجه‌کنید که $\mathcal{S} \neq \varnothing$، زیرا $K \in \mathcal{S}$. مجموعهٔ $\mathcal{S}$ را با تعریف $E_1 \leq E_2$ اگر و فقط اگر E_2 یک توسیع میدان E_1 باشد جزئی مرتب می‌کنیم. تحقیق کنید هر زنجیر در $\mathcal{S}$ کران بالایی دارد (اجتماع میدانها در زنجیر یک نمونه است). بنابراین، طبق لم زرن، عنصر ماکزیمال F از $\mathcal{S}$ وجود دارد.

حکم می‌کنیم که F به‌طور جبری بسته است. چه در غیر این صورت $f \in F[x]$ ی هست که روی F تجزیه‌نمی‌شود. لذا، یک توسیع جبری حقیقی مانند $F_0 = F(u)$ از F وجود دارد، که در آن u ریشه‌ای از f است که در F قرار ندارد (قضیهٔ ۱۰۰۱). به علاوه، طبق

قضیهٔ ۱۳۰۱ ، F_0 توسیع جبری K می‌باشد . بنابراین ، طبق لم ۵۰۳ ،

$$|F_0 - F| \leq |F_0| \leq \aleph_0|K| < |S|$$ و چون $|F| \leq |F_0| < |S|$

$$|S| = |(S - F) \cup F| = |S - F| + |F|$$

باید طبق قضیهٔ ۱۰۰۸ آشنایی داشته باشیم $|S| = |S - F|$. لذا ، $|F_0 - F| < |S - F|$ و نگاشت همانی بر F را می‌توان به‌یک‌نگاشت انژکتیو از مجموعه‌ها مانند $\zeta : F_0 \to S$ توسیع داد . پس $F_1 = \mathrm{Im}\,\zeta$ را می‌توان با تعریف $\zeta(a) + \zeta(b) = \zeta(a + b)$ و $\zeta(a)\zeta(b) = \zeta(ab)$ به یک میدان بدل ساخت . واضح است که F_1 یک توسیع میدان F است ، $F_1 \subset S$ ، و $\zeta : F_0 \to F_1$ یک F ــ یکریختی میدانهاست . درنتیجه ، چون F_0 یک توسیع جبری حقیقی F (و درنتیجه ، K) است ، F_1 نیز چنین خواهد بود . این یعنی $F_1 \in S$ و $F < F_1$ ، که با ماکزیمالی F درتضاداست . بنابراین ، F به‌طورجبری‌بسته بوده و روی K جبری است ؛ و درنتیجه ، یک بسط جبری K می‌باشد . حکم یکتایی قضیه در نتیجهٔ ۹۰۳ زیر ثابت می‌شود .

نتیجهٔ ۷۰۳ . هرگاه K میدان بوده و S مجموعه‌ای از چندجمله‌ایها (از درجهٔ مثبت) در K[x] باشد ، آنگاه یک میدان تجزیه‌گر از S روی K وجود خواهد داشت .

برهان . تمرین .

حال به‌یکتایی میدانهای تجزیه‌گر و بستهای جبری می‌پردازیم . جواب حاصل فوری نتیجهٔ زیر در باب توسیع پذیری یکریختیهاست (ر.ک . قضیهٔ ۸۰۱ و چند تبصرهٔ پیش از آن) .

قضیهٔ ۸۰۳ . فرض کنیم $\sigma : K \to L$ یک یکریختی میدانها ، $S = \{f_i\}$ مجموعه‌ای از چندجمله‌ایها (با درجهٔ مثبت) در $K[x]$ ، و $S' = \{\sigma f_i\}$ مجموعهٔ نظیر از چندجمله‌ایها در $L[x]$ باشد . هرگاه F یک میدان تجزیه‌گر S روی K و M یک میدان تجزیه‌گر S' روی L باشد ، آنگاه σ به یک یکریختی مانند $F \cong M$ توسیع پذیر است .

طرح برهان . ابتدا فرض کنیم S فقط از یک چندجمله‌ای مانند $f \in K[x]$ تشکیل شده باشد

و به استقرا بر $n = [F:K]$ عمل می‌کنیم. هرگاه $n = 1$ ، آنگاه $F = K$ و f روی K تجزیه می‌شود. این ایجاب می‌کند که σf روی L تجزیه می‌شود؛ و درنتیجه، $L = M$. لذا، خود σ یکریختی مطلوب $F = K \xrightarrow{\sigma} L = M$ است. هرگاه $n > 1$ ، آنگاه f باید عامل تحویل‌ناپذیر g از درجهٔ بزرگتر از 1 داشته باشد. فرض کنیم u ریشه‌ای از g در F داشته باشد. تحقیق کنید که σg در $L[x]$ تحویل‌ناپذیر است. هرگاه v ریشه‌ای از σg در M باشد، آنگاه، طبق قضیهٔ ۸.۱ ، σ به یکریختی مانند $\tau : K(u) \cong L(v)$ با خاصیت $\tau(u) = v$ توسیع می‌شود. چون $[K(u):K] = \deg g > 1$ (قضیهٔ ۶.۱) ، باید داشته باشیم $[F:K(u)] < n$ (قضیهٔ ۲.۱) . چون F یک میدان تجزیه‌گر f روی $K(u)$ و M یک میدان تجزیه‌گر σf روی $L(v)$ باشد (تمرین ۲) ، فرض استقرا ایجاب می‌کند که τ به یک یکریختی مانند $F \cong M$ توسیع می‌یابد.

اگر S دلخواه باشد، $\mathcal{S}$ را مرکب از تمام سه‌تاییهای (E,N,τ) می‌گیریم، که در آن E یک میدان میانی F و K ، N یک میدان میانی M و L ، و $\tau : E \to N$ یک یکریختی باشد که σ را توسیع می‌دهد. تعریف می‌کنیم $(E_1,N_1,\tau_1) \leq (E_2,N_2,\tau_2)$ اگر $E_1 \subset E_2$ ، $N_1 \subset N_2$ ، و $\tau_2 | E_1 = \tau_1$. تحقیق کنید که $\mathcal{S}$ یک مجموعهٔ جزئی مرتب ناتهی است که در آن هر زنجیر کران بالایی در $\mathcal{S}$ دارد. بنابر لم زرن، یک عنصر ماکزیمال مانند (F_0,M_0,τ_0) از $\mathcal{S}$ موجوداست. حکم می‌کنیم که $F_0 = F$ و $M_0 = M$ ؛ درنتیجه، $\tau_0 : F \cong M$ توسیع مطلوب σ است. هرگاه $F_0 \neq F$ ، آنگاه $f \in S$ ی روی F_0 تجزیه نمی‌شود. چون تمام ریشه‌های f در F واقعند، F شامل یک میدان تجزیه‌گر مانند F_1 از f روی F_0 می‌باشد. به همین نحو، M شامل یک میدان تجزیه‌گر مانند M_1 از $\tau_0 f = \sigma f$ روی M_0 است. قسمت اول برهان نشان می‌دهد که τ_0 را می‌توان به یک یکریختی مانند $\tau_1 : F_1 \cong M_1$ توسیع داد. اما این یعنی که $(F_1,M_1,\tau_1) \in \mathcal{S}$ و $(F_0,M_0,\tau_0) < (F_1,M_1,\tau_1)$ که با ماکزیمالی (F_0,M_0,τ_0) در تضاد است. اگر $M_0 \neq M$ ، استدلالی مشابه با استفاده از τ_0^{-1} به کار خواهد رفت.

نتیجهٔ ۹.۳ . *فرض کنیم K میدان و S مجموعه‌ای از چندجمله‌ایها (با درجهٔ مثبت) در K[x] باشد. در این صورت، دو میدان تجزیه‌گر از S روی K ، K ــ یکریخت‌اند. بخصوص، هر دو بست جبری K ، K ــ یکریخت می‌باشند.*

طرح برهان. قضیهٔ ۸.۳ را به‌ازای $\sigma = 1_K$ به کار برید. در این صورت، آخرین حکم

نتیجهٔ فوری قضیهٔ ۴.۳ (دو) می‌باشد.

برای توصیف توسیعهای گالوا برحسب میدانهای تجزیه‌گر، ابتدا باید پدیده‌ای را درنظر بگیریم که فقط در حالت میدانهای با مشخص ناصفر رخ می‌دهد. به یاد آورید که هرگاه K یک‌میدان، f یک‌چندجمله‌ای‌ناصفر در $K[x]$، و c ریشه‌ای از f باشد، آنگاه $f = (x-c)^m g(x)$، که در آن $g(c) \neq 0$ و m عدد صحیح مثبتی است که به‌طور منحصر به فرد معین می‌شود. عنصر c، بسته به اینکه $m = 1$ یا $m > 1$، یک ریشهٔ **ساده** یا **چندگانهٔ** f است (ر.ک. ص ۲۵۱).

تعریف ۱۰.۳. فرض کنیم K میدان بوده و $f \in K[x]$ یک‌چندجمله‌ای تحویل‌ناپذیر باشد. گوییم چندجمله‌ای f **جدایی‌پذیر** است اگر، در میدان تجزیه‌گری از f روی K، هر ریشهٔ f ساده باشد.

هرگاه F یک توسیع میدان K بوده و $u \in F$ روی K جبری باشد، آنگاه گوییم u روی K **جدایی‌پذیر** است مشروط براینکه‌چندجمله‌ای تحویل‌ناپذیر آن **جدایی‌پذیر** باشد. هرگاه هر عنصر F روی K جدایی‌پذیر باشد، آنگاه گوییم F **یک توسیع جدایی‌پذیر** K است.

چند تبصره. (یک) درپرتونتیجهٔ ۹.۳ واضح است‌که چندجمله‌ای جدایی‌پذیر $f \in K[x]$ در **هیچ** میدان تجزیه‌گر f روی K ریشهٔ چندگانه ندارد. (دو) قضیهٔ III ۱۰.۶۰ نشان می‌دهدکه یک‌چندجمله‌ای تحویل‌ناپذیر در $K[x]$ جدایی‌پذیر است اگر و فقط اگر مشتقش ناصفر باشد، که از آنجا هر چندجمله‌ای تحویل‌ناپذیر جدایی‌پذیر است اگر $\operatorname{char} K = 0$ (تمرین III ۳.۶۰). *ازاینرو، هرتوسیع میدان‌جبری یک میدان با مشخص ۰ جدایی‌پذیر است.* (سه) در اینجا جدایی‌پذیری فقط برای چندجمله‌ایهای **تحویل‌ناپذیر** تعریف شده است. (چهار) بنابر تعریف ۱۰.۳، یک توسیع میدان جدایی‌پذیر از K لزوماً روی K جبری است. تعریفی از جدایی‌پذیری برای توسیعهای میدان احتمالاً غیرجبری وجوددارد‌که درحالت جبری با این یکی است (بخش VI ۲۰). اما در سراسر این فصل فقط از تعریف ۱۰.۳ استفاده خواهیم کرد.

چند مثال. $x^2 + 1 \in \mathbf{Q}[x]$ جدایی‌پذیر است، زیرا در $\mathbf{C}[x]$، $x^2 + 1 = (x+i)(x-i)$.

از آن‌سو، چندجمله‌ای x^2+1 روی Z_2 ریشهٔ ساده ندارد؛ درواقع، این حتی تحویل‌ناپذیر نیست زیرا، در $Z_2[x]$، $x^2+1=(x+1)^2$.

قضیهٔ ۱۱.۳. *هرگاه F یک توسیع میدان K باشد، آنگاه احکام زیر باهم معادلند:*
(یک) F روی K جبری و گالوا است؛
(دو) F روی K جدایی‌پذیر و F یک میدان تجزیه‌گر روی K برای مجموعه‌ای مانند S از چندجمله‌ایها در K[x] است.
(سه) F یک میدان تجزیه‌گر روی K برای مجموعه‌ای مانند T از چندجمله‌ایهای جدایی پذیر در K[x] است.

چند تبصره. هرگاه F روی K با بعد متناهی باشد، آنگاه احکام (دو) و (سه) را می‌توان کمی قویتر ساخت. بخصوص، (سه) را می‌توان با حکم زیر عوض کرد: F یک میدان تجزیه‌گر روی K برای چندجمله‌ای $f\in K[x]$ است که عوامل تحویل‌ناپذیر آن جدایی‌پذیرند (تمرین ۱۳).

برهان ۱۱.۳. (دو) و (سه) $\Rightarrow$ (یک). هرگاه $u\in F$ دارای چندجمله‌ای تحویل‌ناپذیر f باشد، آنگاه قسمت اول برهان لم ۱۳.۲ (به‌ازای $E=F$) دقیقا "قابل بیان است و نشان می‌دهد که f در $F[x]$ به حاصلضربی از عوامل خطی متمایز تجزیه می‌شود. از اینرو، u روی K جدایی‌پذیر است. فرض کنیم $\{v_i \mid i\in I\}$ پایه‌ای از F روی K بوده و، به‌ازای هر $i\in I$، $f_i\in K[x]$ چندجمله‌ای تحویل‌ناپذیری از v_i باشد. تبصره‌های فوق نشان می‌دهند که هر f_i جدایی‌پذیر است و در $F[x]$ تجزیه می‌شود. بنابراین، F یک میدان تجزیه‌گر روی K برای $S=\{f_i \mid i\in I\}$ می‌باشد.
(سه) $\Rightarrow$ (دو) فرض کنیم $f\in S$ و $g\in K[x]$ یک عامل تحویل‌ناپذیر تکین f باشد. چون f در $F[x]$ تجزیه می‌شود، g باید چندجمله‌ای تحویل‌ناپذیر از $u\in F$ ای باشد. چون F روی K جدایی‌پذیر است، g لزوما" جدایی‌پذیر است. پس نتیجه می‌شود که F یک میدان تجزیه‌گر روی K برای مجموعهٔ T از چندجمله‌ایهای جدایی‌پذیر مرکب از تمام عوامل تحویل‌ناپذیر تکین (در $K[x]$) چندجمله‌ایها در S است (ر.ک. تمرین ۴).
(یک) $\Rightarrow$ (سه) F روی K جبری است، زیرا هر میدان تجزیه‌گر روی K یک توسیع

جبری است. هرگاه $u \in F - K$، آنگاه $u \in K(v_1, \ldots, v_n)$ که در آن، بنابر تعریف میدان تجزیه‌گر و قضیهٔ ۳۰۱ (هفت)، هر v_i یک ریشه از $f_i \in T$ ی است. لذا، $u \in E = K(u_1, \ldots, u_r)$، که در آن u_i ها همهٔ ریشه‌های $f_1, \ldots, f_n$ در F اند. از اینرو، بنابر قضیهٔ ۱۲۰۱، $[E : K]$ متناهی است. چون هر f_i در F تجزیه می‌شود، E یک میدان تجزیه‌گر روی K برای مجموعهٔ متناهی $\{f_1, \ldots, f_n\}$ یا، معادلاً "، $f = f_1 f_2 \cdots f_n$ می‌باشد. حال فرض کنیم قضیه در حالت ابعاد متناهی درست باشد. در این صورت، E روی K گالواست؛ و درنتیجه، $\tau \in \mathrm{Aut}_K E$ ای هست به‌طوری‌که $\tau(u) \neq u$. چون F یک میدان تجزیهٔ T روی E است (تمرین ۲)، بنابر قضیهٔ ۸۰۳، τ به یک خودریختی $\sigma \in \mathrm{Aut}_K F$ توسیع می‌یابد به‌طوری‌که $\sigma(u) = \tau(u) \neq u$. بنابراین، u (که عنصر دلخواهی از $F - K$ بود) در میدان ثابت $\mathrm{Aut}_K F$ نیست؛ یعنی، F روی K گالواست.

استدلال بند پیش نشان می‌دهد که کافی است قضیه را وقتی $[F : K]$ متناهی است ثابت کنیم. در این حالت تعدادی متناهی چندجمله‌ای مانند $g_1, \ldots, g_t \in T$ وجود دارند به‌طوری‌که F یک میدان تجزیه‌گر $\{g_1, \ldots, g_t\}$ روی K است (در غیر این صورت، F روی K بابعدنامتناهی است). به علاوه، طبق لم ۸۰۲، $\mathrm{Aut}_K F$ یک گروه متناهی است. هرگاه K_0 میدان ثابت $\mathrm{Aut}_K F$ باشد، آنگاه، بنابر قضیهٔ آرتین ۱۵۰۲ و قضیهٔ اساسی، F یک توسیع گالوای K_0 یا $[F : K] = |\mathrm{Aut}_K F|$ است. لذا، برای اثبات اینکه F روی K گالواست (یعنی $K = K_0$) کافی است نشان دهیم که $[F : K] = |\mathrm{Aut}_K F|$.

به استقرا بر $n = [F : K]$ عمل می‌کنیم، که در آن حالت $n = 1$ بدیهی است. هرگاه $n > 1$، آنگاه یکی از g_i ها، مثلاً " g_1، از درجهٔ $s > 1$ است (در غیر این صورت، تمام ریشه‌های g_i در K واقعند و $F = K$). فرض کنیم $u \in F$ ریشه‌ای از g_1 باشد؛ پس طبق قضیهٔ ۶۰۱ $[K(u) : K] = \deg g_1 = s$ و تعداد ریشه‌های متمایز g_1 مساوی s است، زیرا g_1 جدایی‌پذیر است. بند دوم برهان لم ۸۰۲ (به‌ازای $L = K$، $M = K(u)$، و $f = g_1$) نشان می‌دهد که یک نگاشت انژکتیو از مجموعهٔ تمام هم‌مجموعه‌های چپ $H = \mathrm{Aut}_{K(u)} F$ در $\mathrm{Aut}_K F$ به مجموعهٔ تمام ریشه‌های g_1 در F وجود دارد که با $\sigma H \mapsto \sigma(u)$ داده می‌شود. بنابراین، $[\mathrm{Aut}_K F : H] \leq s$. اما اگر $v \in F$ ریشهٔ دیگری از g_1 باشد، بنابر نتیجهٔ ۹۰۱، یک یکریختی مانند $\tau : K(u) \cong K(v)$ وجود دارد که $\tau(u) = v$ و $\tau \mid K = 1_K$. چون F یک میدان تجزیه‌گر $\{g_1, \ldots, g_t\}$ روی $K(u)$ و روی $K(v)$ است (تمرین ۲)، τ به یک خودریختی مانند $\sigma \in \mathrm{Aut}_K F$ توسیع می‌یابد که $\sigma(u) = v$

(قضیهٔ ۸.۳) . بنابراین ،هر ریشهٔ g_i نقش هم مجموعه‌ای از H است و $[\mathrm{Aut}_K F : H] = s$. به علاوه ، F یک میدان تجزیه‌گر روی $K(u)$ برای مجموعهٔ تمام عوامل تحویل‌ناپذیر h_i (در $K(u)[x]$) از چندجمله‌ایهای g_i است (تمرین ۴) . هر h_i بوضوح جدایی‌پذیر است ، زیرا g_i ی را عـاد مـی‌کند . چون $[F : K(u)] = n/s < n$ ، فرض استقرا ایجاب می‌کند که $[F : K(u)] = |\mathrm{Aut}_{K(u)} F| = |H|$. بنابراین ،

$$[F : K] = [F : K(u)][K(u) : K] = |H|s = |H|[\mathrm{Aut}_K F : H] = |\mathrm{Aut}_K F|$$

و برهان تمام است .

قضیهٔ ۱۲.۳ (قضیهٔ اساسی تعمیم یافته) . *هرگاه F یک توسیع میدان گالوای جبری از K باشد ،آنگاه تناظر یک به یکی بین مجموعهٔ تمام میدانهای میانی توسیع و مجموعهٔ تمام زیرگروههای بستهٔ گروه گالوای $Aut_K F$ وجود دارد (که با $E \mapsto E' = Aut_E F$ داده می‌شود) به‌طوری‌که*

(دو) F روی هر میدان میانی E گالوا است ،ولی E روی K گالوا است اگر وفقط اگر زیرگروه نظیر E' در $G = Aut_K F$ نرمال باشد ؛ در این حالت G/E' با گروه گالوای $Aut_K E$ از E روی K مساوی (یکریخت) است .

چند تبصره . این قضیه ، که ذیلا " ثابت می‌شود ، را با قضیهٔ ۵.۲ مقایسه کنید . مشابه قسمت (یک) درقضیهٔ اساسی درابعاد نامتناهی درست نیست (تمرین ۱۶) . اگر $[F : K]$ نامتناهی باشد ، همواره زیرگروههایی از $\mathrm{Aut}_K F$ وجود دارند که بسته نیستند . برهان این امر بـــه مطلب زیر از کرول [۶۴] بستگی دارد : وقتی F روی K جبری است ، می‌توان $\mathrm{Aut}_K F$ را به‌یک‌گروه توپولوژیک فشرده چنان تبدیل کرد که یک زیرگروه به‌طور توپولوژیک بسته بـاشد اگر و فقط اگر به مفهوم بخش ۲ بسته باشد (یعنی ، $H = H''$) . به‌آسانی معلوم مـی‌شود کـه هر گروه توپولوژیک فشردهٔ نامتناهی شامل زیرگروهی است که به‌طور توپولوژیک بسته نیست . بحثـی کاملتر ، با چند مثال ، در پی ، ج . مک‌کارتی[1] [۴۰]؛ صفحات ۶۰ تا ۶۳ داده شده است . همچنین ، ر.ک. تمرین ۱۱.۵ در زیر .

برهان ۱۲.۳ . در پرتو قضیهٔ ۷.۲ برای اثبات تناظر یک‌به‌یک کافی است نشان دهیم

1. P. J. McCarthy

هر میدان میانی E بسته است. بنابر قضیهٔ ۱۱۰۳ ، F میدان تجزیه‌گر روی K برای مجموعهٔ T از چندجمله‌ایهای جدایی‌پذیر است. بنابراین ، F یک میدان تجزیه‌گر T روی E نیز هست (تمرین ۲) . از اینرو ، باز طبق قضیهٔ ۱۱۰۳ ، F روی E گالواست؛ یعنی ، E بسته است.

(دو) چون هرمیدان‌میانی E روی K جبری است ، می‌توان با استفاده از بند اول برهان قضیهٔ ۵۰۲ (دو) نشان داد که E روی K گالواست اگر و فقط اگر E' در $\mathrm{Aut}_K F$ نرمال باشد.

هرگاه $E = E''$ روی K گالوا باشد ، درنتیجه E' در $G = \mathrm{Aut}_K F$ نرمال است ، آنگاه طبق لم ۱۱۰۲ ، E یک میدان میانی پایدار است. بنابراین ، لم ۱۴۰۲ ایجاب می‌کند که $G/E' = \mathrm{Aut}_K F/\mathrm{Aut}_E F$ با زیرگروه $\mathrm{Aut}_K E$ مرکب‌ازخودریختیهایی‌که به F توسیع پذیر اند یکریخت‌باشد. اما F یک‌میدان‌تجزیه‌گر روی K است (قضیهٔ ۱۱۰۳)؛ و درنتیجه ، روی E نیز چنین است (تمرین ۲) . بنابراین ، طبق‌قضیهٔ ۸۰۳ واینکه $G/E' \cong \mathrm{Aut}_K E$ ، هر K ــ خودریختی در $\mathrm{Aut}_K E$ به F توسیع می‌یابد.

حال بــه میدانهای تجــزیه‌گر بازگشته و آنها را برحسب خاصیتی که قبلا" در چند مورد به کار رفت مشخص می‌نماییم.

تعریف ۱۳۰۳ . توسیع میدان جبری F از K روی K **نرمال** (یا **توسیع نرمال**) است اگر هر چندجمله‌ای تحویل‌ناپذیر K[x] که در F ریشه داشته باشد در F[x] تجزیه شود.

قضیهٔ ۱۴۰۳ . *هرگاه F یک تــوسیع میــدان جبــری K باشد ، آنگاه احکام زیر باهم معادلند :*

(یک) F روی K نرمال است؛

(دو) F یک میدان تجزیه‌گر روی K برای مجمــوعه‌ای از چندجمله‌ایها در K[x] است؛

(سه) هرگاه $\bar{K}$ یک بســت جبــری K شامل F باشد ، آنــگاه ، به‌ازای هر K ــ تکریختی میدانها مانند $\sigma : F \to \bar{K}$ داریم $\mathrm{Im}\,\sigma = F$ ، درنتیجه σ یک K ــ خودریختی F است.

چند تبصره . قضیه در صورتی که بست جبری $\bar{K}$ در (سه) با یک توسیع نرمال K شامل

F عوض شود برقرار می‌ماند (تمرین ۲۱) . برای برهان سرراستی از (یک) $\Rightarrow$ (دو) در ابعاد متناهی ، ر.ک. تمرین ۲۵ .

برهان ۱۴۰۳ . (دو) $\Rightarrow$ (یک) F یک میدان تجزیه‌گر روی K برای $\{f_i \in K[x] \mid i \in I\}$ است ، که در آن $\{u_i \mid i \in I\}$ یک پایهٔ F روی K بوده و f_i چندجمله‌ای تحویل‌ناپذیری از u_i است .

(سه) $\Rightarrow$ (دو) فرض کنیم F یک‌میدان‌تجزیه‌گراز $\{f_i \mid i \in I\}$ روی K بوده‌و $\sigma : F \to \bar{K}$ یک K ــ تکریختی میدانها باشد . هرگاه $u \in F$ ریشه‌ای از f_i باشد ، آنگاه $\sigma(u)$ نیزچنین است (همان برهان قضیهٔ ۲۰۲) . طبق فرض، f_i در F تجزیه می‌شود؛ مثلا "، $f_i = c(x-u_1)\cdots(x-u_n)$ $(u_i \in F; c \in K)$. چون $\bar{K}[x]$ یک دامنهٔ یکتایی تجزیه است (نتیجهٔ III ۴۰۶۰) ، به‌ازای هر i ، $\sigma(u_i)$ یکی از $u_1, \ldots, u_n$ است (ر.ک. قضیهٔ III ۶۰۶۰) . چون σ انژکتیو است ، باید u_i را جایگشت دهد . اما F روی K به وسیلهٔ تمام‌ریشه‌های‌جمیع f_i ها تولیدمی‌شود . پس ازقضیهٔ ۳۰۱ نتیجه می‌شود که $\sigma(F) = F$ ؛ و درنتیجه ، $\sigma \in \mathrm{Aut}_K F$.

(یک) $\Rightarrow$ (سه) فرض کنیم $\bar{K}$ یک بست جبری F باشد (قضیهٔ ۶۰۳) . پس $\bar{K}$ روی K جبری است (قضیهٔ ۱۳۰۱) . بنابر این ، $\bar{K}$ یک بست جبری K شامل F است (قضیهٔ ۴۰۳) . فرض کنیم $f \in K[x]$ تحویل‌ناپذیر با ریشهٔ $u \in F$ باشد . بنابر ساخت ، $\bar{K}$ شامل تمام ریشه‌های f است . هرگاه $v \in \bar{K}$ ریشه‌ای از f باشد ، آنگاه یک K ــ یکریختی از میدانها مانند $\sigma : K(u) \cong K(v)$ باخاصیت $\sigma(u) = v$ وجود دارد (نتیجهٔ ۹۰۱) که ، بنابر قضایای ۴۰۳ و ۸۰۳ و تمرین ۲ ، به یک K ــ خودریختی از $\bar{K}$ توسیع می‌یابد . $\sigma \mid F$ یک تکریختی $F \to \bar{K}$ است و ، بنابه فرض، $\sigma(F) = F$. بنابراین، $v = \sigma(u) \in F$ ، کهایجاب می‌کند f در F تجزیه‌می‌شود . ازاینرو ، F روی K نرمال است .

نتیجهٔ ۱۵۰۳ . *فرض کنیم F یک توسیع میدان جبری K باشد . در این صورت ، F روی K گالوا است اگر و فقط اگر F روی K نرمال و جدایی‌پذیر باشد . هرگاه* $\mathrm{char}\, K = 0$ ، *آنگاه F روی K گالوا است اگر و فقط اگر F روی K نرمال باشد .*

برهان . تمرین؛ از قضایای ۱۱۰۳ و ۱۴۰۳ استفاده کنید .

قضیهٔ ۱۶۰۳ . هرگاه E یک توسیع میدان جبری از K باشد ، آنگاه یک توسیع میدان F از E وجود دارد به‌طوری‌که

(یک) F روی K نرمال است ؛

(دو) هیچ زیرمیدان حقیقی F شامل E روی K نرمال نیست ؛

(سه) هرگاه E روی K جدایی‌پذیر باشد ، آنگاه F روی K گالوا است ؛

(چهار) $[F:K]$ متناهی است اگر و فقط اگر $[E:K]$ متناهی باشد .

میدان F با تقریب یک E ــ یکریختی به‌طور منحصر به فرد معین می‌شود .

میدان F در قضیهٔ ۱۶۰۳ را گاهی **بست نرمال** E روی K می‌نامند .

برهان ۱۶۰۳ . (یک) فرض کنیم $X = \{u_i \mid i \in I\}$ پایه‌ای از E روی K بوده و $f_i \in K[x]$ چندجمله‌ای تحویل‌ناپذیری از u_i باشد . هرگاه F یک میدان تجزیه‌گر $S = \{f_i \mid i \in I\}$ روی E باشد ،آنگاه F یک میدان تجزیه‌گر S روی K نیز هست (تمرین ۳) ، که از آنجا ، طبق قضیهٔ ۱۴۰۳ ، F روی K نرمال است . هرگاه E روی K جدایی‌پذیر باشد ، آنگاه‌هر f_i جدایی‌پذیر است . بنابراین ،طبق قضیهٔ ۱۱۰۳ ، F روی K گالواست . (چهار) هرگاه $[E:K]$ متناهی باشد ، آنگاه X ، و درنتیجه ، S نیز متناهی است . این ایجاب می‌کند که (بنابر تبصره‌های بعد از تعریف ۱۰۳) $[F:K]$ متناهی باشد . (دو) زیرمیدان F_0 از F که شامل E باشد لزوما" حاوی ریشهٔ u_i از $f_i \in S$ به‌ازای هر i است . هرگاه F_0 روی K نرمال باشد (درنتیجه ، طبق تعریف ، هر f_i در F_0 تجزیه می‌شود) ، آنگاه $F \subset F_0$ ؛ و درنتیجه ، $F = F_0$.

بالاخره ، فرض کنیم F_1 توسیع میدان دیگری از E با خواص (یک) و (دو) باشد . چون F_1 روی K نرمال و شامل هر u_i است ، F_1 باید شامل میدان‌تجزیه‌گری مانند F_2 از S روی K باخاصیت $E \subset F_2$ باشد . F_2 روی K نرمال‌است (قضیهٔ ۱۴۰۳) ، که‌ازآنجا ، طبق (دو) ، $F_2 \simeq F_1$. بنابراین ، هر دوی F و F_1 میدانهای تجزیه‌گری از S روی K ، و درنتیجه از S روی E ، می‌باشند (تمرین ۲) . بنابر قضیهٔ ۸۰۳ ، نگاشت همانی بر E به یک E ــ یکریختی مانند $F \cong F_1$ توسیع می‌یابد .

ضمیمه: قضیهٔ اساسی جبر

قضیهٔ مذکوردر عنوان می‌گوید که میدان اعداد مختلط $\mathbf{C}$ به‌طور جبری بسته است (یعنی ،

هر معادلهٔ چندجمله‌ای روی $\mathbf{C}$ را می‌توان کاملا" حل کرد.) هر برهان شناخته شده از این امر جایی به نتایجی از آنالیز بستگی دارد. فرض این است که

(آ) هر عدد حقیقی مثبت دارای ریشهٔ دوم مثبت حقیقی است؛

(ب) هرچندجمله‌ای در $\mathbf{R}[x]$ از درجهٔ فرد در $\mathbf{R}$ ریشه دارد (یعنی، هرچندجمله‌ای تحویل‌ناپذیر در $\mathbf{R}[x]$ از درجهٔ بزرگتر از یک با درجهٔ زوج است).

فرض (آ) از ساختن اعداد حقیقی از اعداد گویا نتیجه می‌شود و فرض (ب) نتیجه‌ای از قضیهٔ مقدار میانی در حساب دیفرانسیل و انتگرال مقدماتی می‌باشد؛ ر.ک. تمرین III ۱۶۰۶۰. مطلب را با اثبات حالت خاصی از یک قضیه که ذیلا" مطرح می‌شود (حکم ۱۵۰۶) آغاز می‌کنیم.

لم ۱۷۰۳. *هرگاه F یک توسیع جدایی‌پذیر با بعد متناهی از میدان نامتناهی K باشد، آنگاه، به‌ازای $u \in F$ ای، $F = K(u)$.*

طرح برهان. بنابر قضیهٔ ۱۶۰۳، یک توسیع میدان گالوا با بعد متناهی مانند F_1 از K وجود دارد که شامل F است. قضیهٔ اساسی ۵۰۲ ایجاب می‌کند که $\mathrm{Aut}_K F_1$ متناهی است و توسیع K به وسیلهٔ F_1 فقط تعدادی متناهی میدان میانی دارد. بنابراین، فقط می‌توان تعدادی متناهی میدان میانی در توسیع K به‌وسیلهٔ F داشت.

چون $[F : K]$ متناهی است، می‌توان $u \in F$ را چنان یافت که $[K(u) : K]$ ماکزیمال باشد. اگر $K(u) \neq F$، $v \in F - K(u)$ ای وجود دارد. تمام میدانهای میانی به شکل $K(u + av)$، که $a \in K$، را درنظر می‌گیریم. چون K نامتناهی است و فقط تعدادی متناهی میدان میانی وجود دارد، $a, b \in K$ ای وجود دارند به‌طوری‌که $a \neq b$ و $K(u + av) = K(u + bv)$. بنابراین، $(a - b)v = (u + av) - (u + bv) \in K(u + av)$. چون $a \neq b$، داریم $v = (a - b)^{-1}(a - b)v \in K(u + av)$، که از آنجا

$$u = (u + av) - av \in K(u + av).$$

درنتیجه، $K \subset K(u) \subsetneq K(u + av)$، که از آنجا $[K(u + av) : K] > [K(u) : K]$. این با انتخاب u تعارض دارد. ازاینرو، $K(u) = F$.

لم ۱۸۰۳. *هیچ توسیع میدانی با بعد 2 روی میدان اعداد مختلط وجود ندارد.*

طرح برهان. به آسانی معلوم می‌شود که هر توسیع میدان F با بعد 2 روی $\mathbf{C}$ لزوماً، به‌ازای $u \in F - \mathbf{C}$، به شکل $F = C(u)$ است. بنابرقضیهٔ ۶۰۱، u ریشهٔ یک چندجمله‌ای تکین تحویل‌ناپذیر $f \in \mathbf{C}[x]$ از درجهٔ 2 است. برای اتمام برهان، کافی است نشان دهیم چنین f ی نمی‌تواند وجود داشته باشد.

بنابرفرض (آ) به‌ازای هر $a + bi \in \mathbf{C} = \mathbf{R}(i)$، اعداد حقیقی مثبت $|(a + \sqrt{a^2 + b^2})/2|$ و $|(-a + \sqrt{a^2 + b^2})/2|$ به‌ترتیب دارای ریشه‌های دوم مثبت حقیقی c و d اند. تحقیق کنیدکه، با انتخاب‌مناسب علامتها، $(\pm c \pm di)^2 = a + bi$. از اینرو، هر عنصر $\mathbf{C}$ ریشهٔ دومی در $\mathbf{C}$ دارد. درنتیجه، هرگاه $f = x^2 + sx + t \in \mathbf{C}[x]$، آنگاه f دارای ریشه‌های $(-s \pm \sqrt{s^2 - 4t})/2$ در $\mathbf{C}$ است، که از آنجا f روی $\mathbf{C}$ تجزیه می‌شود. لذا، چندجمله‌ای تکین تحویل‌ناپذیری از درجهٔ 2 در $\mathbf{C}[x]$ وجود ندارد.

قضیهٔ ۱۹۰۳ (قضیهٔ اساسی جبر). *میدان اعداد مختلط به‌طور جبری بسته است.*

برهان. برای آنکه نشان دهیم هر $f \in \mathbf{C}[x]$ غیرثابت‌روی $\mathbf{C}$ تجزیه می‌شود، بنابر قضیهٔ ۱۰۰۱ کافی است ثابت کنیم $\mathbf{C}$ جز خود توسیع با بعد متناهی ندارد. چون $[\mathbf{C} : \mathbf{R}] = 2$ و $\text{char } \mathbf{R} = 0$، هر توسیع میدان با بعد متناهی E_1 از $\mathbf{C}$ یک توسیع جدایی‌پذیر با بعد متناهی $\mathbf{R}$ است (قضیهٔ ۲۰۱). درنتیجه، بنابر قضیهٔ ۱۶۰۳، E_1 مشمول یک توسیع میدان گالوا بابعد متناهی مانند F از $\mathbf{R}$ است. برای به دست آوردن $E_1 = \mathbf{C}$ کافی است نشان دهیم $F = \mathbf{C}$.

قضیهٔ اساسی ۵۰۲ نشان می‌دهد که $\text{Aut}_{\mathbf{R}}F$ یک گروه متناهی است. بنابر قضایای II ۷۰۵۰ و ۵۰۲، $\text{Aut}_{\mathbf{R}}F$ یک 2 ـ زیرگروه زیلوف مانند H از مرتبهٔ 2^n $(n \geq 0)$ و با اندیس فرد دارد، که میدان ثابت E آن بابعد فرداست $[E : \mathbf{R}] = [\text{Aut}_{\mathbf{R}}F : H]$. E روی $\mathbf{R}$ جدایی‌پذیر است (زیرا $\text{char } \mathbf{R} = 0$)، کهازآنجا، طبق لم ۱۷۰۳، $E = \mathbf{R}(u)$. لذا، چندجمله‌ای تحویل‌ناپذیر u دارای درجهٔ فرد $[E : \mathbf{R}] = [\mathbf{R}(u) : \mathbf{R}]$ است (قضیهٔ ۶۰۱). این درجه باید، طبق فرض (ب)، مساوی 1 باشد. بنابراین، $u \in \mathbf{R}$ و $[\text{Aut}_{\mathbf{R}}F : H] = [E : \mathbf{R}] = 1$، که از آنجا $\text{Aut}_{\mathbf{R}}F = H$ و $|\text{Aut}_{\mathbf{R}}F| = 2^n$. درنتیجه، زیرگروه $\text{Aut}_{\mathbf{C}}F$ از $\text{Aut}_{\mathbf{R}}F$، به‌ازای m ی $(0 \leq m \leq n)$، از مرتبهٔ 2^m است.

فرض کنیم $m > 0$. طبق قضیهٔ اول زیلوف II ۷۰۵۰، $\text{Aut}_{\mathbf{C}}F$ زیرگروهی چون

J با اندیس 2 دارد؛ فرض کنیم E_0 میدان ثابت J باشد. بنابر قضیهٔ اساسی، E_0 یک توسیع $\mathbf{C}$ با بعد $[\mathrm{Aut}_{\mathbf{C}}F : J] = 2$ است، که با لم ۱۸.۳ متناقض است. بنابراین، $m = 0$ و $\mathrm{Aut}_{\mathbf{C}}F = 1$. قضیهٔ اساسی ۵.۲ ایجاب می‌کند که $[F : \mathbf{C}] = [\mathrm{Aut}_{\mathbf{C}}F : 1] = |\mathrm{Aut}_{\mathbf{C}}F| = 1$، که از آنجا $F = \mathbf{C}$.

نتیجهٔ ۲۰.۳. *هر توسیع میدان جبری حقیقی از میدان اعداد حقیقی با میدان اعداد مختلط یکریخت است.*

برهان. هرگاه F یک توسیع جبری $\mathbf{R}$ بوده و $u \in F - \mathbf{R}$ دارای چندجمله‌ای تحویل‌ناپذیر $f \in R[x]$ از درجهٔ بزرگتر از یک باشد، آنگاه، طبق قضیهٔ ۱۹.۳، f روی $\mathbf{C}$ تجزیه می‌شود. هرگاه $v \in \mathbf{C}$ ریشه‌ای از f باشد، آنگاه، طبق نتیجهٔ ۹.۱، نگاشت همانی بر $\mathbf{R}$ به یک یکریختی مانند $\mathbf{R}(u) \cong \mathbf{R}(v) \subset \mathbf{C}$ توسیع می‌یابد. چون $[\mathbf{R}(v) : \mathbf{R}] = [\mathbf{R}(u) : \mathbf{R}] > 1$ و $[\mathbf{C} : \mathbf{R}] = 2$، باید داشته باشیم $[\mathbf{R}(v) : \mathbf{R}] = 2$ و $\mathbf{R}(v) = \mathbf{C}$. بنابراین، F یک توسیع جبری میدان به‌طور جبری بستهٔ $\mathbf{R}(u) \cong \mathbf{C}$ است. اما یک میدان به‌طور جبری بسته جز خود توسیع جبری ندارد (قضیهٔ ۳.۳). لذا، $F = \mathbf{R}(u) \cong \mathbf{C}$.

تمرینات

تذکر. F همواره یک توسیع میدان از میدان K بوده و S مجموعه‌ای از چندجمله‌ایها (از درجهٔ مثبت) در $K[x]$ است مگر خلافش گفته شود.

۱. F یک میدان تجزیه‌گر روی K برای مجموعهٔ متناهی $\{f_1, \ldots, f_n\}$ از چندجمله‌ایها در $K[x]$ است اگر و فقط اگر F میدان تجزیه‌گر چندجمله‌ای $f = f_1 f_2 \cdots f_n$ روی K باشد.

۲. هرگاه F میدان تجزیه‌گر S روی K و E میدان میانی باشد، آنگاه F میدان تجزیه‌گر S روی E است.

۳. (آ) فرض کنید E میدان میانی توسیع $K \subset F$ بوده و $E = K(u_1, \ldots, u_r)$، که در آن u_i ها (بعضی از) ریشه‌های $f \in K[x]$ اند. در این صورت، F یک میدان تجزیه‌گر f روی K است اگر و فقط اگر F یک میدان تجزیه‌گر f روی E باشد.
(ب) قسمت (آ) را به میدانهای تجزیه‌گر مجموعه‌های دلخواه از چندجمله‌ایها

تعمیم دهید.

۴. هرگاه F یک میدان تجزیه‌گر S روی K باشد، آنگاه F نیز یک میدان تجزیه‌گر روی K برای مجموعهٔ T متشکل‌ازتمام‌عوامل‌تحویل‌ناپذیر از چندجمله‌ایها در S است.

۵. هرگاه $f \in K[x]$ از درجهٔ n بوده و F یک میدان تجزیه‌گر f روی K باشد، آنگاه $[F:K]$ ، $n!$ را عاد می‌کند.

۶. فرض کنید K چنان میدانی باشد که، به‌ازای هر توسیع میدان F ، توسیع جبری ماکزیمال K مشمول F (ر.ک. قضیهٔ ۱۴۰۱) خود K است. در این صورت، K به‌طور جبری بسته است.

۷. هرگاه F به‌طور جبری بسته بوده و E از تمام عناصری در F تشکیل شده باشد که روی K جبری‌اند، آنگاه E یک‌بست‌جبری K خواهد بود [ر.ک. قضیهٔ ۱۴۰۱].

۸. هیچ‌میدان‌متناهی K به‌طورجبری‌بسته‌نیست. [**راهنمایی.** اگر $K = \{a_0, \dots, a_n\}$ ، $a_1 + (x - a_0)(x - a_1)\cdots(x - a_n) \in K[x]$ را، که در آن $a_1 \neq 0$ ، درنظر بگیرید.]

۹. F یک بست جبری K است اگر و فقط اگر F روی K جبری بوده و، به‌ازای هر بست جبری E از K ، یک K ــ تکریختی مانند $E \to F$ وجود داشته باشد.

۱۰. F یک بست جبری K است اگر و فقط اگر F روی K جبری بوده و، به‌ازای هر توسیع میدان جبری E از میدان دیگر K_1 و یکریختی $\sigma : K_1 \to K$ از میدانها، σ به یک تکریختی مانند $E \to F$ توسیع یابد.

۱۱. (آ) هرگاه $u_1, \dots, u_n \in F$ روی K جدایی‌پذیر باشند، آنگاه $K(u_1, \dots, u_n)$ یک توسیع جدایی‌پذیر K می‌باشد.

(ب) هرگاه F به وسیلهٔ مجموعه‌ای (احتمالاً نامتناهی) از عناصر جدایی‌پذیر روی K تولید شده باشد، آنگاه F یک توسیع جدایی‌پذیر K می‌باشد.

۱۲. فرض کنید E یک میدان میانی باشد.

(آ) هرگاه $u \in F$ روی K جدایی‌پذیر باشد، آنگاه u روی E جدایی‌پذیر است.

(ب) هرگاه F روی K جدایی‌پذیرباشد، آنگاه F روی E و E روی K جدایی‌پذیر است.

۱۳. فرض کنید $[F:K]$ متناهی باشد. در این صورت، شرایط زیر باهم معادلند:

(یک) F روی K گالوا است؛

(دو) F روی K جدایی‌پذیر و یک میدان تجزیه‌گر $f \in K[x]$ است؛

(سه) F یک میدان تجزیه‌گر روی K برای چندجمله‌ای $f \in K[x]$ است که عوامل تحویل‌ناپذیرش جدایی‌پذیرند.

۱۴. (قضیهٔ لاگرانژ در باب گنگیهای طبیعی). هرگاه L و M میدانهایی میانی باشند به‌طوری‌که L یک توسیع گالوای با بعد متناهی K باشد، آنگاه LM با بعد متناهی و گالوا روی M بوده و $\mathrm{Aut}_M LM \cong \mathrm{Aut}_{L\cap M} L$.

۱۵. فرض کنید E یک میدان میانی باشد.

(آ) هرگاه F روی K گالوای جبری باشد، آنگاه F روی E گالوای جبری است. [تمرینات ۹۰۲ و ۱۱۰۲ نشان می‌دهند که فرض "جبری بودن" ضرورت دارد.]

(ب) هرگاه F روی E و E روی K گالوا بوده، و F یک میدان تجزیه‌گر روی E برای خانواده‌ای از چندجمله‌ایها در $K[x]$ باشد، آنگاه F روی K گالوا خواهد بود [ر.ک. تمرین ۱۲۰۲].

۱۶. فرض کنید F یک بسط جبری میدان اعداد گویای $\mathbf{Q}$ بوده و $E \subset F$ یک میدان تجزیه‌گر روی $\mathbf{Q}$ برای مجموعهٔ $S = \{x^2 + a \mid a \in \mathbf{Q}\}$ باشد؛ درنتیجه، E روی $\mathbf{Q}$ جبری و گالوا می‌باشد (قضیهٔ ۱۱۰۳).

(آ) $E = \mathbf{Q}(X)$ ، که درآن $X = \{\sqrt{p} \mid p = -1$ یا p عدد صحیح اولی است$\}$.

(ب) هرگاه $\sigma \in \mathrm{Aut}_{\mathbf{Q}} E$ ، آنگاه $\sigma^2 = 1_E$. بنابراین، گروه $\mathrm{Aut}_{\mathbf{Q}} E$ عملاً "یک‌فضای برداری روی Z_2 است [ر.ک. تمرینات I ۱۳۰۱۰ و IV ۱۰۱۰].

(پ) $\mathrm{Aut}_{\mathbf{Q}} E$ نامتناهی است و شمارشپذیر نیست. [**راهنمایی.** بهازای هر زیرمجموعهٔ Y از X، $\sigma \in \mathrm{Aut}_{\mathbf{Q}} E$ ای وجود دارد به‌طوری‌که $\sigma(\sqrt{p}) = -\sqrt{p}$ بهازای $\sqrt{p} \in Y$ و $\sigma(\sqrt{p}) = \sqrt{p}$ بهازای $\sqrt{p} \in X - Y$. بنابراین، طبق آشنایی، قضیهٔ ۵۰۸، $|\mathrm{Aut}_{\mathbf{Q}} E| = |P(X)| > |X|$. اما $|X| = \aleph_0$.]

(ت) هرگاه B پایه‌ای از $\mathrm{Aut}_{\mathbf{Q}} E$ روی Z_2 باشد، آنگاه B نامتناهی است و شمارشپذیر نیست.

(ث) $\mathrm{Aut}_{\mathbf{Q}} E$ تعدادی شمارش‌ناپذیر نامتناهی زیرگروه با اندیس 2 دارد. [**راهنمایی.** هرگاه $b \in B$، آنگاه $B - \{b\}$ زیرگروهی با اندیس 2 تولید می‌کند.]

(ج) مجموعهٔ توسیعهای میدان $\mathbf{Q}$ مشمول E با بعد 2 روی $\mathbf{Q}$ شمارشپذیراست.

(چ) مجموعهٔ زیرگروههای بسته با اندیس 2 در $\mathrm{Aut}_{\mathbf{Q}} E$ شمارشپذیر است.

(ح) $[E : \mathbf{Q}] \leq \aleph_0$ ، که از آنجا $[E : \mathbf{Q}] < |\mathrm{Aut}_{\mathbf{Q}} E|$.

۱۷ . هرگاه میدان میانی E روی K نرمال باشد، آنگاه E (نسبت به F و K) پایدار است.

۱۸ . فرض کنید F روی K نرمال بوده و E یک میدان میانی باشد. در این صورت، E روی K نرمال است اگر و فقط اگر E پایدار باشد [ر.ک. تمرین ۱۷]. به علاوه، $\mathrm{Aut}_K F/E' \cong \mathrm{Aut}_K E$.

۱۹ . قسمت (دو) یا (دوُ) قضیهٔ اساسی (۵۰۲ یا ۱۲۰۳) معادل حکم زیر است: میدان میانی E روی K نرمال است اگر و فقط اگر زیرگروه نظیر E' در $G = \mathrm{Aut}_K F$ نرمال باشد، که در این صورت $G/E' \cong \mathrm{Aut}_K E$. [ر.ک. تمرین ۱۸]

۲۰ . هرگاه F روی میدان میانی E و E روی K نرمال باشد، آنگاه F لزوماً روی K نرمال نیست. [**راهنمایی.** فرض کنید $\sqrt[4]{2}$ ریشهٔ چهارم حقیقی 2 بوده و $\mathbf{Q}(\sqrt[4]{2}) \supset \mathbf{Q}(\sqrt{2}) \supset \mathbf{Q}$ را درنظر بگیرید؛ از تمرین ۲۳ استفاده کنید.] با تمرین ۲ مقایسه کنید.

۲۱ . فرض کنید F روی K جبری باشد. F روی K نرمال است اگر و فقط اگر به‌ازای هر K ــ تکریختی میدانها مانند $\sigma : F \to N$ ، که در آن N توسیع نرمالی از K شامل F است، $\sigma(F) = F$ ؛ درنتیجه، σ یک K ــ خودریختی F است.
[**راهنمایی.** از برهان قضیهٔ ۱۴۰۳ با استفاده از قضیهٔ ۱۶۰۳ تقلید کنید.]

۲۲ . هرگاه F روی K جبری بوده و هر عنصر F متعلق به یک میدان میانی باشد که روی K نرمال است، آنگاه F روی K نرمال می‌باشد.

۲۳ . هرگاه $[F : K] = 2$ ، آنگاه F روی K نرمال است.

۲۴ . توسیع جبری F از K روی K نرمال است اگر و فقط اگر به‌ازای هر $f \in K[x]$ تحویل‌ناپذیر، f به‌صورت حاصلضربی از عوامل تحویل‌ناپذیر در $F[x]$ تجزیه شود که تمام آنها از درجهٔ یکسان باشند.

۲۵ . فرض کنید F یک میدان تجزیه‌گر $f \in K[x]$ باشد. با استفاده از قضیهٔ ۱۴۰۳ ، نشان دهید F روی K نرمال است. [**راهنماییها.** هرگاه عنصر تحویل‌ناپذیر $g \in K[x]$ دارای ریشهٔ $u \in F$ باشد ولی در F تجزیه نشود، آنگاه نشان دهید یک K ــ یکریختی مانند $\varphi : K(u) \cong K(v)$ وجود دارد، که در آن $v \notin F$ و v ریشه‌ای از g است. نشان دهید که φ به یک یکریختی مانند $F \cong F(v)$ توسیع می‌یابد. این رابطهٔ $[F : K] < [F(v) : K]$ را نقض می‌کند.]

۴ گروه گالوای یک چندجمله‌ای

هدف اصلی این بخش ذکر چند کاربرد و مثال از مفاهیم بخشهای پیش است. این مطالب درآینده، جز در دو مورد، به کار نمی‌آیند. تعریف ۱۰۴ و قضیهٔ ۱۲۰۴، که فقط به قضیهٔ ۲۰۴ وابسته‌اند، در بخش ۹ که حلپذیری به‌وسیلهٔ رادیکالها برای یک معادلهٔ چندجمله‌ای مطرح می‌شود، به کار خواهند رفت.

تعریف ۱۰۴. فرض کنیم K یک میدان باشد. *گروه گالوای چندجمله‌ای* $f \in K[x]$ گروه $Aut_K F$ است، که در آن F یک میدان تجزیه‌گر f روی K است.

به خاطر نتیجهٔ ۹۰۳، گروه گالوای f از انتخاب F مستقل است. پیش از ذکر مثال، ابتدا چند مطلب مفید عرضه می‌کنیم. به یاد آورید که زیرگروه G از گروه متقارن S_n **متعدی** است اگر به‌ازای هر $i \neq j$ $(1 \leq i,j \leq n)$، $\sigma \in G$ ای موجود باشد به‌طوری‌که $\sigma(i) = j$.

قضیهٔ ۲۰۴. *فرض کنیم K میدان بوده و $f \in K[x]$ یک چندجمله‌ای با گروه گالوای G باشد.*

(یک) G با زیرگروهی از یک گروه متقارن S_n یکریخت است.

(دو) هرگاه f (تحویل‌ناپذیر) جدایی‌پذیر از درجهٔ n باشد، آنگاه n، $|G|$ را عاد می‌کند و G با یک زیرگروه متعدی S_n یکریخت است.

طرح برهان. (یک) هرگاه $u_1, \ldots, u_n$ ریشه‌های متمایزی از f در میدان تجزیه‌گر F باشد $(1 \leq n \leq \deg f)$، آنگاه قضیهٔ ۲۰۲ ایجاب می‌کند که هر $\sigma \in \mathrm{Aut}_K F$ یک جایگشت منحصر به فرد از $\{u_1, \ldots, u_n\}$ را القا می‌نماید (ولی عکس این لزوماً برقرار نیست!). S_n را گروه تمام جایگشتهای $\{u_1, \ldots, u_n\}$ گرفته و تحقیق کنید که انتساب $\sigma \in \mathrm{Aut}_K F$ به جایگشتی که القا می‌کند یک تکریختی مانند $\mathrm{Aut}_K F \to S_n$ تعریف می‌کند. (توجه کنید که $F = K(u_1, \ldots, u_n)$.)

(دو) F روی K گالواست (قضیهٔ ۱۱۰۳) و $[K(u_1) : K] = n = \deg f$ (قضیهٔ ۶۰۱). بنابراین، طبق قضیهٔ اساسی ۵۰۲، G زیرگروهی با اندیس n دارد، که از آنجا $n \mid |G|$.

بـه‌ازای هـر $i \neq j$ ، یک K ــ یکریختی مانند $\sigma : K(u_i) \cong K(u_j)$ وجود دارد به‌طوری‌که $\sigma(u_i) = u_j$ (نتیجهٔ ۹۰۱) . بنـابر قضیـهٔ ۸۰۳ ، σ به یک K ــ خودریختی F توسیع می‌یابد، که از آنجا G با زیرگروهی متعدی از S_n یکریخت است .

از حالا به‌بعد گروه گالوای چندجمله‌ای f را اغلب با زیرگروه یکریخت با آن از S_n یکی کرده و آن را گروهی از جایگشتهای ریشه‌های f درنظر می‌گیریم . به علاوه ، عمدتا" با چندجمله‌ایهای $f \in K[x]$ کارمی‌کنیم‌که تمام ریشه‌هـایش در میدان تجزیه‌گری متمایزند . این‌ایجاب می‌کندکه عوامل تحویل‌ناپذیر f جدایی‌پذیرند . درنتیجه ، طبق قضیهٔ ۱۱۰۳ (و تمرین ۱۳۰۳) ، میدان تجزیه‌گر F از f روی K گالواست . هرگاه گروههای گالوای این چندجمله‌ایها همیشه قابل محاسبه باشند ، آنگاه می‌توان (دست‌کم در اصول) گروه گالوای یک چندجمله‌ای دلخواه را حساب کرد (تمرین ۱) .

نتیجهٔ ۳۰۴ . فرض‌کنیم K یک میـدان بوده و $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر از درجهٔ 2 با گروه گالوای G باشد . هـرگاه f جدایی‌پذیر باشد (که همواره در صورت $char\, K \neq 2$ چنین است) ، آنگاه $G \cong Z_2$ ؛ در غیر این صورت ، $G = 1$.

طرح برهان . توجه کنید که $S_2 = Z_2$. از تبصـرهٔ (دو) بعد از تعریف ۱۰۰۳ و قضیهٔ ۲۰۴ استفاده کنید .

از قضیهٔ ۲۰۴ (دو) فورا" نتیجه می‌شود که گروه گالوای یک چندجمله‌ای جدایی‌پذیر از درجهٔ 3 یا S_3 است یا A_3 (تنها زیـرگروههـای متعدی S_3) . برای به دست آوردن نتیجه‌ای قویتر ، تعریف کلیتری می‌آوریم .

تعریف ۴۰۴ . فرض‌کنیم K میدانی با $char\, K \neq 2$ بوده‌و $f \in K[x]$ یک چندجمله‌ای از درجهٔ n با n ریشهٔ متمایز $u_1, \ldots, u_n$ در میدان‌تجزیه‌گر F از f روی Kباشد.همچنین ، $\Delta = \prod_{i<j} (u_i - u_j) = (u_1 - u_2)(u_1 - u_3)\cdots(u_{n-1} - u_n) \in F$ ؛مبین f عنصر $D = \Delta^2$می‌باشد.

توجه کنید که Δ عنصری از میدان تجزیه‌گر خاصی چون F است ؛ و لذا ، **به طریق**

اولی، $D = \Delta^2$ نیز در F است. با اینحال، داریم.

حکم ۵۰۴. فرض کنیم K، f، F، و Δ همانند در تعریف ۴۰۴ باشند.
(یک) مبین Δ^2 ی f عملا" در K قرار دارد.
(دو) به‌ازای هر $\sigma \in Aut_K F < S_n$، σ یک جایگشت زوج [فرد] است اگر و فقط اگر $\sigma(\Delta) = \Delta$ [$\sigma(\Delta) = -\Delta$].

طرح برهان. در مورد (دو)، ر.ک. برهان قضیهٔ I ۷۰۶۰. با فرض (دو) می‌بینیم که به‌ازای هر $\sigma \in Aut_K F$، $\sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = \Delta^2$. بنابراین، $\Delta^2 \in K$، زیرا F روی K گالواست (قضیهٔ ۱۱۰۳؛ تمرین ۱۳۰۳).

نتیجهٔ ۶۰۴. *فرض کنیم K, f, F, Δ همانند در تعریف ۴۰۴ باشند (درنتیجه، F روی K گالواست) و $G = Aut_K F$ را زیرگروهی از S_n می‌گیریم. در تناظر گالوا (قضیهٔ ۵۰۲) زیرمیدان $K(\Delta)$ نظیر زیرگروه $G \cap A_n$ است. بخصوص، G متشکل از جایگشتهای زوج است اگر و فقط اگر $\Delta \in K$.*

برهان. تمرین.

نتیجهٔ ۷۰۴. *فرض کنیم K یک میدان بوده و $f \in K[x]$ یک چندجمله‌ای جدایی‌پذیر (تحویل‌ناپذیر) از درجهٔ 3 باشد. گروه گالوای f یا S_3 است یا A_3. اگر $char\, K \neq 2$، مساوی A_3 است اگر و فقط اگر مبین f مربع عنصری از K باشد.*

برهان. تمرین؛ از قضیهٔ ۲۰۴ و نتیجهٔ ۶۰۴ استفاده کنید.

هرگاه میدان پایهٔ K زیرمیدانی از میدان اعداد حقیقی باشد، آنگاه با استفاده از مبین چندجمله‌ای مکعبی $f \in K[x]$ می‌توان تعداد ریشه‌های حقیقی f را یافت (تمرین ۲).

فرض کنیم f همانند در نتیجهٔ ۷۰۴ باشد. اگر گروه گالوای f مساوی $A_3 \cong Z_3$ باشد، البته میدان میانی وجود نخواهد داشت. هرگاه مساوی S_3 باشد، آنگاه چهار میدان

میانی حقیقی $K(\Delta)$ ، $K(u_1)$ ، $K(u_2)$ ، و $K(u_3)$ وجوددارند ،که در آنها u_1,u_2,u_3 ریشه‌های f اند . $K(\Delta)$ نظیر A_3 و $K(u_i)$ نظیرزیرگروه $\{(1),(jk)\}$ $(i \neq j,k)$ از S_3 است ،که‌از مرتبهٔ 2 و اندیس 3 می‌باشد (تمرین ۳) .

پس جز در حالت مشخص 2 ، محاسبهٔ گروه گالوای یک مکعبی جدایی‌پذیر به محاسبهٔ مبین و تعیین اینکه مربعی در K هست یا نه تحویل می‌شود . نتیجهٔ زیر گاهی مفید واقع خواهد شد .

حکم ۸۰۴ . فرض کنیم K میدانی با $\mathrm{char}\ K \neq 2,3$ باشد . هرگاه

$$f(x) = x^3 + bx^2 + cx + d \in K[x]$$

سه ریشهٔ متمایز درمیدانی تجزیه‌گرداشته باشد ، آنگاه چندجمله‌ای $g(x) = f(x - b/3) \in K[x]$ **به شکل** $x^3 + px + q$ **بوده و مبین** f **خواهد بود** $-4p^3 - 27q^2$.

طرح برهان . فرض کنید F یک میدان تجزیه‌گر f روی K باشد و تحقیق کنید $u \in F$ ریشهٔ f است‌اگرو فقط اگر $u + b/3$ ریشه‌ای از $g = f(x - b/3)$ باشد . این ایجاب می‌کند که g همان مبین f راداشته باشد .تحقیق کنید g به شکل $x^3 + px + q$ $(p,q \in K)$ است. فرض کنید v_1,v_2,v_3 ریشه‌های g در F باشند . دراین صورت ،

$$(x - v_1)(x - v_2)(x - v_3) = g(x) = x^3 + px + q$$

که ایجاب می‌کند که

$$\begin{aligned} &v_1 + v_2 + v_3 = 0;\\ &v_1v_2 + v_1v_3 + v_2v_3 = p;\\ &-v_1v_2v_3 = q. \end{aligned}$$

چون هر v_i ریشه‌ای از g است ،

$$v_i^3 = -pv_i - q \qquad (i = 1,2,3).$$

این امر که مبین Δ^2 از g مساوی $-4p^3 - 27q^2$ است‌ازیک محاسبهٔ طولانی مستلزم تعریف $\Delta^2 = (v_1 - v_2)^2(v_1 - v_3)^2(v_2 - v_3)^2$ ، معادلهٔ فوق ، و اینکه $(v_i - v_j)^2 = (v_i + v_j)^2 - 4v_iv_j$ نتیجه خواهد شد .

مثال . چندجمله‌ای $x^3 - 3x + 1 \in \mathbf{Q}[x]$ ، طبق قضیهٔ III ۶۰۶۰ وحکم III ۸۰۶۰ ، تحویل‌ناپذیر است و جدایی‌پذیر است زیرا $\mathrm{char}\ \mathbf{Q} = 0$. مبین مساوی است با

$-4(-3)^3 - 27(1)^2 = 108 - 27 = 81$ ، که در $\mathbf{Q}$ مربع است. از اینرو، طبق نتیجهٔ ۷.۴، گروه گالوا مساوی A_3 است.

مثال. هرگاه $f(x) = x^3 + 3x^2 - x - 1 \in \mathbf{Q}[x]$، آنگاه

$$g(x) = f(x - 3/3) = f(x - 1) = x^3 - 4x + 2,$$

که طبق محک آیزنشتاین (قضیهٔ III ۱۵.۶۰) تحویل‌ناپذیر است. بنابر حکم ۸.۴، مبین f مساوی است با $-4(-4)^3 - 27(2)^2 = 256 - 108 = 148$ که در $\mathbf{Q}$ مربع نیست. بنابراین، گروه گالوا مساوی S_3 می‌باشد.

حال به‌چندجمله‌ایها از درجهٔ چهار (درجهٔ چهارها) روی میدان K می‌پردازیم. همانندفوق، فقط به آن $f \in K[x]$ هایی خواهیم پرداخت که در میدان تجزیه‌گر F ریشه‌های متمایز u_1,u_2,u_3,u_4 را دارند. درنتیجه، F روی K گالوا بوده و می‌توان گروه گالوای f را گروهی از جایگشتهای $\{u_1,u_2,u_3,u_4\}$ و زیرگروهی از S_4 درنظر گرفت. زیرمجموعهٔ $V = \{(1),(12)(34),(13)(24),(14)(23)\}$ یک زیرگروه نرمال S_4 است (تمرین ۷.۶۰ I)، که نقش مهمی در بحث دارد. توجه کنید که V با گروه چهارگان $Z_2 \oplus Z_2$ یکریخت است و $V \cap G$ زیرگروه‌نرمال $G = \mathrm{Aut}_K F < S_4$ می‌باشد.

لم ۹.۴. فرض کنیم K، f، F، u_i، V، و $G = Aut_K F < S_4$ **همانند در بند پیش باشند. هرگاه** $\alpha = u_1u_2 + u_3u_4$، $\beta = u_1u_3 + u_2u_4$، $\gamma = u_1u_4 + u_2u_3 \in F$، **آنگاه، تحت‌تناظرگالوا (قضیهٔ ۵.۲)، زیرمیدان** $K(\alpha,\beta,\gamma)$ **نظیر زیرگروه نرمال** $V \cap G$ **می‌باشد. از اینرو،** $K(\alpha,\beta,\gamma)$ **روی** K **گالواست و** $Aut_K K(\alpha,\beta,\gamma) \cong G/(G \cap V)$.

طرح برهان. واضح است که هر عنصر در $G \cap V$، α,β,γ، و درنتیجه $K(\alpha,\beta,\gamma)$، را ثابت می‌گذارد. برای تکمیل برهان، به خاطر قضیهٔ اساسی، کافی است نشان دهیم که هر عنصر G غیرواقع در V دست‌کم یکی از α,β,γ را حرکت می‌دهد. مثلاً"، هرگاه $\sigma = (12) \in G$ و $\sigma(\beta) = \beta$، آنگاه $u_2u_3 + u_1u_4 = u_1u_3 + u_2u_4$؛ و درنتیجه، $u_2(u_3 - u_4) = u_1(u_3 - u_4)$. لذا، $u_1 = u_2$ یا $u_3 = u_4$، که هر یک تناقض است. بنابراین، $\sigma(\beta) \neq \beta$. حالات دیگر به همین نحو ثابت می‌شوند. [**راهنمایی.** به جای امتحان

کردن همهٔ 20 حالت، نشان دهید کافی است برای هر هم‌مجموعهٔ V در S_4 فقط یک نماینده درنظر گرفته شود] .

فرض کنیم K, f, F, u_i و α,β,γ همانند درلم ۹.۴ باشند . عناصر α,β,γ نقش قاطعی در تعیین گروههای گالوای درجه چهارهای دلخواه ایفا می‌کنند . چندجمله‌ای $(x-\alpha)(x-\beta)(x-\gamma) \in K(\alpha,\beta,\gamma)[x]$ **مکعبی حلال** f نام دارد . مکعبی حلال عملا" یک چندجمله‌ای روی $\mathbf{K}$ است :

لم ۱۰.۴ . هرگاه K یک میدان بوده و $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$ ، آنگاه مکعبی حلال f چندجمله‌ای $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$ می‌باشد .

طرح برهان . فرض کنیم f دارای ریشه‌های $u_1, \ldots, u_4$ درمیدان تجزیه‌گری چون F باشد. با استفاده از $f = (x-u_1)(x-u_2)(x-u_3)(x-u_4)$ ، u_i را برحسب b,c,d,e بیان کنید . مکعبی حلال $(x-\alpha)(x-\beta)(x-\gamma)$ را بسط داده از جانشانیهای مناسب ، تعریف α,β,γ (لم ۹.۴) ، و عبارات مربوط به b,c,d,e به دست آمده درفوق استفاده نمایید .

حال در وضعی هستیم که گروه گالوای هر چندجمله‌ای درجهٔ چهار جدایی‌پذیر (تحویل‌ناپذیر) $f \in K[x]$ را حساب کنیم . چون گروه گالوای G آن یک زیرگروه متعدی S_4 می‌باشد که مرتبه‌اش بر 4 بخشپذیر است (قضیهٔ ۲.۴) ، G باید دارای مرتبهٔ 24 ، 12 ، 8 ، یا 4 باشد . تحقیق کنید که تنها زیرگروههای متعدی مراتب 24 ، 12 ، و 4 عبارتند از S_4 ، A_4 ، $V (\cong Z_2 \oplus Z_2)$ ، و گروههای دوری مختلف از مرتبهٔ 4 که به وسیلهٔ 4 ــ دورها تولید می‌شوند ؛ ر.ک. تمرین I ۵.۴۰ و قضیهٔ I ۸.۶۰ . یک زیرگروه متعدی S_4 از مرتبهٔ 8 گروه دووجهی D_4 تولید شده به وسیلهٔ (1234) و (24) است (صفحهٔ ۷۸) . چون D_4 در S_4 نرمال نیست ، و چون هر زیرگروه از مرتبهٔ 8 یک 2 ــ زیرگروه زیلوف است ، پس از قضایای دوم و سوم زیلوف نتیجه می‌شود که S_4 دقیقا" سه زیرگروه از مرتبهٔ 8 دارد ، که هر یک با D_4 یکریخت است .

حکم ۱۱.۴ . فرض کنیم K یک میدان و $f \in K[x]$ یک درجهٔ چهار جدایی‌پذیر

(تحویل‌ناپذیر) با گروه گالوای G *(به عنوان زیرگروهی از* S_4 *) باشد. همچنین،* α,β,γ *ریشه‌های مکعبی حلال* f *بوده و* $m = [K(\alpha,\beta,\gamma) : K]$ *. در این صورت،*

(یک) $m = 6 \Leftrightarrow G = S_4$ ؛

(دو) $m = 3 \Leftrightarrow G = A_4$ ؛

(سه) $m = 1 \Leftrightarrow G = V$ ؛

(چهار) $G \cong Z_4$ یا $G \cong D_4$ $m = 2 \Leftrightarrow G \cong D_4$ ؛ *در این حالت،* $G \cong D_4$ *اگر* f *روی* $K(\alpha,\beta,\gamma)$ *تحویل‌ناپذیر است و* $G \cong Z_4$ *در غیر این صورت.*

طرح برهان. چون $K(\alpha,\beta,\gamma)$ یک میدان تجزیه‌گر یک چندجمله‌ای مکعبی روی K است، تنها امکان برای m عبارت است از 1 ، 2 ، 3 ، و 6 . در پرتو این امر و بحث پیش از قضیه، کافی است استلزام $\Leftarrow$ در هر حالت ثابت شود. از این استفاده می‌کنیم که، طبق لم ۹۰۴ ، $m = [K(\alpha,\beta,\gamma) : K] = |G/G \cap V|$.

هرگاه $G = A_4$ ، آنگاه $G \cap V = V$ و $m = |G/V| = |G|/|V| = 3$. به همین نحو، هرگاه $G = S_4$ ، آنگاه $m = 6$. هرگاه $G = V$ ، آنگاه $G \cap V = G$ و $m = |G/G| = 1$. هرگاه $G \cong D_4$ ، آنگاه $G \cap V = V$ ، زیرا V مشمول هر 2 ــ زیرگروه زیلوف S_4 است و $m = |G/V| = |G|/|V| = 2$.هرگاه G دوری از مرتبهٔ 4 باشد، آنگاه G با یک 4 ــ دور تولید می‌شود که مربعش باید در V باشد؛ درنتیجه، $|G \cap V| = 2$ و $m = |G/G \cap V| = |G|/|G \cap V| = 2$.

چون f تحویل‌ناپذیر یا تحویل‌پذیر است و $D_4 \ncong Z_4$ ، کافی است عکس حکم اخیر را ثابت کنیم. فرض کنیم u_1,u_2,u_3,u_4 ریشه‌های f در میدان تجزیه‌گر F بوده و $G \cong D_4$ ؛ درنتیجه، داریم $G \cap V = V$.چون V یک زیرگروه متعدی بوده و $G \cap V = \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$ (لم ۹۰۴) ، به‌ازای هر جفت $i \neq j$ $(1 \leq i,j \leq 4)$ یک $\sigma \in G \cap V$ وجود دارد که به یک یک‌ریختی مانند $K(\alpha,\beta,\gamma)(u_i) \cong K(\alpha,\beta,\gamma)(u_j)$ تحویل می‌شود به‌طوری‌که $\sigma(u_i) = u_j$ و $\sigma \mid K(\alpha,\beta,\gamma)$ همانی است. لذا، طبق نتیجهٔ ۹۰۱ ، به‌ازای هر $i \neq j$ ، u_i و u_j ریشه‌های یک چندجمله‌ای تحویل‌ناپذیر روی $K(\alpha,\beta,\gamma)$ می‌باشند. پس نتیجه می‌شود که f روی $K(\alpha,\beta,\gamma)$ تحویل‌ناپذیر است. از آن سو، هرگاه $G \cong Z_4$ ، آنگاه $G \cap V = \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$ دارای مرتبهٔ 2 بوده و متعدی نمی‌باشد. از اینرو، به‌ازای $i \neq j$ ای، $\sigma \in G \cap V$ ای وجود ندارد که $\sigma(u_i) = u_j$. اما چون F میدان تجزیه‌گری روی $K(\alpha,\beta,\gamma)(u_i)$ و

$K(\alpha,\beta,\gamma)(u_i)$ است، اگر یک یکریختی مانند $K(\alpha,\beta,\gamma)(u_i) \cong K(\alpha,\beta,\gamma)(u_j)$ وجود می‌داشت که بر $K(\alpha,\beta,\gamma)$ همانی بوده و u_i را به u_j می‌برد، بنابر قضیهٔ ۸.۳، تحدید $\sigma \in \mathrm{Aut}_{K(\alpha,\beta,\gamma)}F = G \cap V$ ای می‌بود. بنابراین، یک چنین یکریختی وجود ندارد، که از آنجا، طبق نتیجهٔ ۹.۱، u_i و u_j نمی‌توانند ریشه‌های چند جمله‌ای تحویل‌ناپذیر واحدی روی $K(\alpha,\beta,\gamma)$ باشند. درنتیجه، f باید روی $K(\alpha,\beta,\gamma)$ تحویل‌پذیر باشد.

مثال. بنابر محک آیزنشتاین (قضیهٔ III ۱۵.۶۰)، چند جمله‌ای $f = x^4 + 4x^2 + 2 \in \mathbf{Q}[x]$ تحویل‌ناپذیر است؛ f جدایی‌پذیر است، چراکه داریم $\mathbf{Q} = 0$. با استفاده از لم ۱۰.۴، مکعبی حلال مساوی $(x^2 - 8)(x - 4) = x^3 - 4x^2 - 8x + 32$ به دست می‌آید؛ درنتیجه، $\alpha = 4$، $\beta = \sqrt{8}$، $\gamma = -\sqrt{8}$ و $\mathbf{Q}(\alpha,\beta,\gamma) = \mathbf{Q}(\sqrt{8}) = \mathbf{Q}(2\sqrt{2}) = \mathbf{Q}(\sqrt{2})$ بعد 2 روی $\mathbf{Q}$ است. ازاینرو، گروه گالوا مساوی (یکریخت با) D_4 یا Z_4 است. جانشانی $z = x^2$، f را به $z^2 + 4z + 2$ تحویل می‌کند، که به آسانی می‌بینیم ریشه‌هایش $z = -2 \pm \sqrt{2}$ می‌باشند؛ لذا، ریشه‌های f عبارتند از $x = \pm\sqrt{z} = \pm\sqrt{-2 \pm \sqrt{2}}$. ازاینرو،

$$f = (x - \sqrt{-2 + \sqrt{2}})(x + \sqrt{-2 + \sqrt{2}})(x - \sqrt{-2 - \sqrt{2}})(x + \sqrt{-2 - \sqrt{2}})$$
$$= (x^2 - (-2 + \sqrt{2}))\,(x^2 - (-2 - \sqrt{2})) \in \mathbf{Q}(\sqrt{2})[x].$$

بنابراین، f روی $\mathbf{Q}(\sqrt{2})$ تحویل‌پذیر است؛ و درنتیجه، طبق حکم ۱۱.۴ (چهار)، گروه گالوا دوری از مرتبهٔ 4 می‌باشد.

مثال. برای یافتن گروه گالوای $f = x^4 - 10x^2 + 4 \in \mathbf{Q}[x]$، ابتدا تحقیق می‌کنیم که f تحویل‌ناپذیر (و لذا، جدایی‌پذیر) است. f در $\mathbf{Q}$ ریشه ندارد؛ و لذا، طبق قضیهٔ III ۶.۶۰ و حکم III ۸.۶۰، عاملی خطی یا مکعبی نخواهد داشت. برای تحقیق در عوامل درجهٔ دوم، بنابرلم III ۱۳.۶۰، کافی است نشان دهیم f در $\mathbf{Z}[x]$ عامل درجهٔ دوم ندارد. به آسانی تحقیق می‌شود که اعداد صحیحی مانند a,b,c,d وجود ندارند که $f = (x^2 + ax + b)(x^2 + cx + d)$. لذا، f در $\mathbf{Q}[x]$ تحویل‌ناپذیر است. مکعبی حلال f مساوی $(x + 10)(x + 4)(x - 4) = x^3 + 10x^2 - 16x - 160$ است، که جمیع ریشه‌هایش در $\mathbf{Q}$ اند. بنابراین، طبق حکم ۱۱.۴، $m = [\mathbf{Q}(\alpha,\beta,\gamma) : \mathbf{Q}] = 1$ و گروه گالوای f مساوی $V\ (\cong Z_2 \oplus Z_2)$ می‌باشد.

مثال . بنابر محک آیزنشتاین ، چندجمله‌ای $x^4 - 2 \in \mathbf{Q}[x]$ تحویل‌ناپذیر (و جدایی‌پذیر) است. مکعبی حلال مساوی است با $\mathbf{Q}(\alpha,\beta,\gamma) = \mathbf{Q}(\sqrt{2}i)$ و $x^3 + 8x = x(x + 2\sqrt{2}i)(x - 2\sqrt{2}i)$ با بعد 2 روی $\mathbf{Q}$ است . تحقیق کنید که $x^4 - 2$ روی $\mathbf{Q}(\sqrt{2}i)$ تحویل‌ناپذیر است (زیرا $\sqrt{2}, \sqrt[4]{2} \notin \mathbf{Q}(\sqrt{2}i)$) . بنابراین ، طبق حکم ۱۱.۴ ، گروه گالوا با گروه دووجهی D_4 یکریخت است .

مثال . چندجمله‌ای $f = x^4 - 5x^2 + 6 \in \mathbf{Q}[x]$ را درنظر می‌گیریم . توجه کنید که f روی $\mathbf{Q}$ تحویل‌پذیر است ؛ یعنی ، $f = (x^2 - 2)(x^2 - 3)$. لذا ، حکم ۱۱.۴ در اینجا قابل اعمال نیست . واضح است که $F = \mathbf{Q}(\sqrt{2},\sqrt{3})$ یک میدان تجزیه‌گر f روی $\mathbf{Q}$ است ، و چون $x^2 - 3$ روی $\mathbf{Q}(\sqrt{2})$ تحویل‌ناپذیر است ، $[F : \mathbf{Q}] = [F : \mathbf{Q}(\sqrt{2})]\,[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2 \cdot 2 = 4$. بنابراین ، طبق قضیهٔ اساسی ، $\mathbf{Aut}_{\mathbf{Q}}F$ ، یعنی گروه گالوای f ، از مرتبهٔ 4 می‌باشد . پس ازبرهان قضیهٔ ۲.۴ و نتیجهٔ ۳.۴ معلوم می‌شود که $\mathbf{Aut}_{\mathbf{Q}}\mathbf{Q}(\sqrt{2})$ از دو عنصر تشکیل شده است ، نگاشت همانی و نگاشت σ که $\sigma(\sqrt{2}) = -\sqrt{2}$. بنابر نتیجهٔ ۹.۱ ، هر یک از 1 و σ به دو راه مختلف (بسته به اینکه $\sqrt{3} \mapsto \sqrt{3}$ یا $\sqrt{3} \mapsto -\sqrt{3}$) به یک $\mathbf{Q}$ ـ خودریختی F توسیع می‌یابد . این امر چهار عنصر متمایز از $\mathbf{Aut}_{\mathbf{Q}}F$ (که به‌وسیلهٔ چهارترکیب ممکن تعیین می‌شوند : $\sqrt{2} \mapsto \pm\sqrt{2}$ و $\sqrt{3} \mapsto \pm\sqrt{3}$) به دست می‌دهد . چون $|\mathbf{Aut}_{\mathbf{Q}}F| = 4$ و هریک ازاین خودریختیها از درجهٔ 2 است ، گروه گالوای f باید ، بنابر تمرین I ۵.۴۰ ، با گروه چهارگان $Z_2 \oplus Z_2$ یکریخت باشد .

تعیین میدانهای‌میانی‌و زیرگروههای نظیرگروه گالوای یک درجهٔ چهار جدایی‌پذیر از انجام این کار برای‌یک مکعبی جدایی‌پذیر مشکلتر است . ازجمله ممکن است ، ولو $u_i \neq u_j$ ، داشته باشیم $K(u_i) = K(u_j)$ (ر.ک. آخرین مثال دربالا) . هیچ حکمی با بیان ساده وجود ندارد که حالت درجهٔ چهار را بپوشاند و به هر وضع باید جداگانه پرداخته شود .

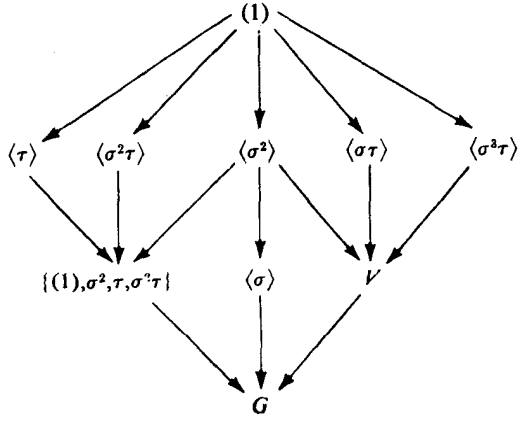
مثال . فرض کنیم $F \subset \mathbf{C}$ یک‌میدان‌تجزیه‌گر از $f = x^4 - 2 \in \mathbf{Q}[x]$ روی $\mathbf{Q}$ باشد . هرگاه u ریشهٔ چهارم حقیقی مثبت 2 باشد ، آنگاه ریشه‌های f عبارتند از $u, -u, ui, -ui$. برای آنکه گروه گالوای $G = \mathbf{Aut}_{\mathbf{Q}}F$ از f را زیرگروهی از S_4 بگیریم ، باید به ریشه‌ها ترتیبی بدهیم ؛ مثلا " $u_1 = u, u_2 = -u, u_3 = ui, u_4 = -ui$ ، . از مثال سوم بعد از حکم

۱۱.۴ می‌دانیم که G یکی از سه زیرگروه از مرتبهٔ 8 در S_4 است، که هر یک با گروه دووجهی D_4 یکریخت می‌باشد. توجه کنید که تزویج مختلط یک $\mathbf{R}$ ــ خودریختی از $\mathbf{C}$ است که بوضوح $u \mapsto u$ ، $-u \mapsto -u$ ، $ui \mapsto -ui$ ، و $-ui \mapsto ui$. لذا، یک $\mathbf{Q}$ ــ خودریختی مانند τ از $F = \mathbf{Q}(u,ui)$ را القا می‌کند. به عنوان عنصری از S_4 ، $\tau = (34)$. اما هر زیرگروه از مرتبهٔ 8 در S_4 با D_4 مزدوج است (قضیهٔ دوم زیلوف) و محاسبه‌ای ساده نشان می‌دهد که تنها زیرگروه شامل (34) زیرگروه D است که به وسیلهٔ $\sigma = (1324)$ و $\tau = (34)$ تولیدمی‌شود. به‌آسانی معلوم می‌شود که $F = \mathbf{Q}(u,ui) = \mathbf{Q}(u,i)$ ؛ درنتیجه، هر $\mathbf{Q}$ ــ خودریختی F کاملا" با عملش بر u و i معین می‌شود. لذا، عناصر D را می‌توان برحسب σ و τ یا عملشان بر u و i توصیف کرد. این اطلاعات در جدول زیر خلاصه شده‌اند:

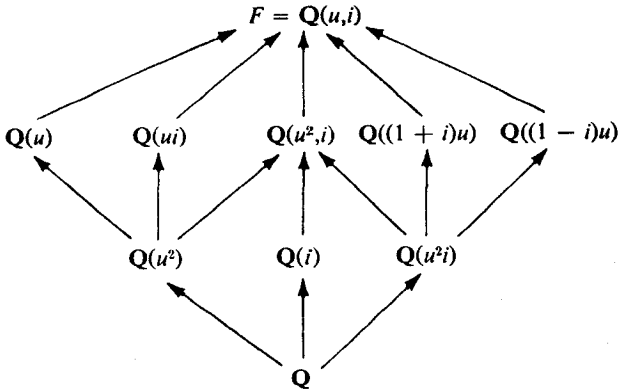
	(1)	(34) τ	(1324) σ	(12)(34) σ^2	(1423) σ^3	(13)(24) $\sigma\tau$	(12) $\sigma^2\tau$	(14)(23) $\sigma^3\tau$
$u \mapsto$	u	u	ui	$-u$	$-ui$	ui	$-u$	$-ui$
$i \mapsto$	i	$-i$	i	i	i	$-i$	$-i$	$-i$

بر خواننده است تحقیق کند که شبکهٔ زیرگروهی D و شبکهٔ میدانهای میانی به صورت زیرند، که در تناظرگالوا میدانها و زیرگروهها وضعیت نظیری نسبت به هم دارند.

شبکهٔ زیرگروهی ($H < K$ یعنی $H \to K$):



شبکهٔ میدان میانی ($M \subset N$ یعنی $M \to N$):



برای محاسبهٔ گروههای گالوای چندجمله‌ایها از درجهٔ بزرگتر از 4 روی میدانهای دلخواه مشخصی وجود دارند. ما به حالت بسیار خاص زیر قانعیم.

قضیهٔ ۱۲.۴. *هرگاه p اول بوده و f یک چندجمله‌ای تحویل‌ناپذیر از درجهٔ p روی میدان اعداد گویا باشد که در میدان اعداد مختلط درست دو ریشهٔ غیرحقیقی دارد، آنگاه گروه گالوای f مساوی (یکریخت با) S_p است.*

طرح برهان. فرض کنیم G گروه گالوای f به‌عنوان زیرگروهی از S_p باشد. چون $p \mid |G|$ (قضیهٔ ۲.۴)، بنابر قضیهٔ کشی II ۲.۵۰، G شامل عنصری مانند σ از مرتبهٔ p است. بنابرنتیجهٔ I ۴.۶۰، σ یک p ــ دور است. اما تزویج مختلط $(a + bi \mapsto a - bi)$ یک $\mathbf{R}$ ــ خودریختی $\mathbf{C}$ است که هر عنصر غیرحقیقی را حرکت می‌دهد. بنابراین، طبق قضیهٔ ۲.۲، دو ریشهٔ غیرحقیقی f را باهم عوض کرده و سایرین را ثابت می‌گذارد. این ایجاب می‌کند که G شامل ترانهش $\tau = (ab)$ باشد. چون σ را می‌توان به صورت $\sigma = (aj_2 \cdots j_p)$ نوشت، توانی از σ به شکل $\sigma^k = (abi_3 \cdots i_p) \in G$ می‌باشد. با تغییر نمادگذاری، در صورت لزوم، می‌توان فرض کرد $\tau = (12)$ و $\sigma^k = (123 \cdots p)$. اما، بنابر تمرین I ۴.۶۰، این دو عنصر S_p را تولید می‌کنند. بنابراین، $G = S_p$.

مثال. بررسی نمودار $f = x^5 - 4x + 2 \in \mathbf{Q}[x]$ نشان می‌دهد که آن فقط سه ریشهٔ حقیقی دارد. بنابر محک آیزنشتاین (قضیهٔ III ۱۵.۶۰)، چندجمله‌ای f تحویل‌ناپذیر است

و ، طبق قضیهٔ ۱۲.۴ ، گروه گالوای آن S_5 می‌باشد .

هنوز به این امر که آیا ، به‌ازای هر گروه متناهی G ، یک توسیع میدان گالوای $\mathbf{Q}$ با گروه گالوای G وجود دارد یا نه پاسخ داده نشده است . اما ، اگر $G = S_n$ ، جواب مثبت می‌باشد (تمرین ۱۴) .

تمرینات

تذکر. K یک میدان است ، $f \in K[x]$ ، و F یک میدان تجزیه‌گر f روی K است مگر خلافش گفته شود .

۱ . فرض کنید $f \in K[x]$ در F به صورت $f = (x-u_1)^{n_1}\cdots(x-u_k)^{n_k}$ تجزیه‌شود (u_i ها متمایزند ؛ $n_i \geq 1$) . فرض کنید $v_0, \ldots, v_k$ ضرایب چند جمله‌ای $g = (x-u_1)(x-u_2)\cdots(x-u_k)$ بوده و نیز $E = K(v_0, \ldots, v_k)$ در این صورت ،

(آ) F یک میدان تجزیه‌گر g روی E است ؛

(ب) F روی E گالوا است ؛

(پ) $\mathrm{Aut}_E F = \mathrm{Aut}_K F$.

۲ . فرض کنید K زیرمیدانی از $\mathbf{R}$ بوده (درنتیجه ، F را می‌توان زیر میدانی از $\mathbf{C}$ گرفت) و f تحویل‌ناپذیر از درجهٔ 3 باشد . همچنین ، D مبین f باشد . در این صورت ،

(آ) $D > 0$ اگر و فقط اگر f سه ریشهٔ حقیقی داشته باشد ؛

(ب) $D < 0$ اگر و فقط اگر f درست یک ریشهٔ حقیقی داشته باشد .

۳ . فرض کنید f یک‌مکعبی جدایی‌پذیر با گروه گالوای S_3 و ریشه‌های $u_1, u_2, u_3 \in F$ باشد . در این صورت ، میدانهای میانی متمایز توسیع K به وسیلهٔ F عبارتند از $F, K(\Delta), K(u_1), K(u_2), K(u_3), K$. زیرگروههای نظیر گروه گالوا عبارتند از 1 ، A_3 ، T_1 ، T_2 ، T_3 ، و S_3 ، که $T_i = \{(1), (jk) \mid j \neq i \neq k\}$.

۴ . هرگاه $\mathrm{char}\, K \neq 2, 3$ ، آنگاه مبین $x^3 + bx^2 + cx + d$ مساوی است با $-4c^3 - 27d^2 + b^2(c^2 - 4bd) + 18bcd$.

۵ . هرگاه $\mathrm{char}\, K \neq 2$ و $f \in K[x]$ یک مکعبی باشد که مبین آن در K مربع است ، آنگاه f یا تحویل‌ناپذیر است یا کاملا " در K تجزیه می‌شود .

۶ . $x^3 - 3x + 1$ روی هر میدان پایهٔ K یا تحویل‌ناپذیر است یا تجزیه می‌شود .

۷ . S_4 زیرگروه متعدی از مرتبهٔ 6 ندارد .

۸ . فرض کنید f یک درجهٔ چهـــــار جدایی‌پذیر (تحویل‌ناپذیر) روی K بـــوده و u ریشه‌ای از f باشد . میدانی حقیقتا" بین K و $K(u)$ وجود ندارد اگر و فقط اگر گروه گالوای f مساوی A_4 یا S_4 باشد .

۹ . فرض کنید $x^4 + ax^2 + b \in K[x]$ (با $\text{char } K \neq 2$) تحویل‌ناپذیر با گروه گالوای G باشد .

(آ) هرگاه b در K مربع باشد ، آنگاه $G = V$.

(ب) هرگاه b در K مربع نبوده و $b(a^2 - 4b)$ در K مربع باشد ، آنگاه $G \cong Z_4$.

(پ) هرگاه نه b و نه $b(a^2 - 4b)$ در K مربع نباشد ، آنگاه $G \cong D_4$.

۱۰ . گروههای گالوای چندجمله‌ایهای زیر را روی میدانهای ذکر شده تعیین کنید .

(آ) $x^4 - 5$ روی $\mathbf{Q}$ ؛ روی $\mathbf{Q}(\sqrt{5})$ ؛ روی $\mathbf{Q}(\sqrt{5}i)$.

(ب) $(x^3 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7)$ روی $\mathbf{Q}$.

(پ) $x^3 - x - 1$ روی $\mathbf{Q}$ ؛ روی $\mathbf{Q}(\sqrt{23}i)$.

(ت) $x^3 - 10$ روی $\mathbf{Q}$ ؛ روی $\mathbf{Q}(\sqrt{2})$.

(ث) $x^4 + 3x^3 + 3x - 2$ روی $\mathbf{Q}$.

(ج) $x^5 - 6x + 3$ روی $\mathbf{Q}$.

(چ) $x^3 - 2$ روی $\mathbf{Q}$.

(ح) $(x^3 - 2)(x^2 - 5)$ روی $\mathbf{Q}$.

(خ) $x^4 - 4x^2 + 5$ روی $\mathbf{Q}$.

(د) $x^4 + 2x^2 + x + 3$ روی $\mathbf{Q}$.

۱۱ . تمام زیرگروههای گـروه گـالوا و تمام میدانهای میانی میدان تجزیه‌گر (روی $\mathbf{Q}$) چندجمله‌ای $(x^3 - 2)(x^2 - 3) \in \mathbf{Q}[x]$ را تعیین کنید .

۱۲ . فرض کنید K زیـرمیدانی از اعـداد حقیقـی بـوده و $f \in K[x]$ یک درجـهٔ چهار تحویل‌ناپذیر بـاشد . اگر f درست دو ریشهٔ حقیقی داشته باشد ، گروه گالوای f مساوی S_4 یا D_4 است .

۱۳ . فرض کنید $f(x) \in K[x]$ دارای ریشه‌های متمایز $u_1, u_2, \ldots, u_n$ در میدان تجزیه‌گر F بوده و $G = \text{Aut}_K F < S_n$ گـروه گـالوای f باشد . همچنین ، $y_1, \ldots, y_n$ مجهولات

بوده و تعریف کنید :

$$g(x) = \prod_{\sigma \in S_n} (x - (u_{\sigma(1)}y_1 + u_{\sigma(2)}y_2 + \cdots + u_{\sigma(n)}y_n)) .$$

(آ) نشان دهید که

$$g(x) = \prod_{\sigma \in S_n} (x - (u_1 y_{\sigma(1)} + u_2 y_{\sigma(2)} + \cdots + u_n y_{\sigma(n)})).$$

(ب) نشان دهید که $g(x) \in K[y_1, \ldots, y_n, x]$.

(پ) فرض کنید $g(x)$ به صورت $g_1(x)g_2(x)\cdots g_r(x)$ تجزیه شود ، که در آن $g_i(x) \in K(y_1, \ldots, y_n)[x]$ تحویل‌ناپذیر تکین است . هرگاه $x - \sum_i u_{\sigma(i)}y_i$ عاملی از $g_1(x)$ باشد ، آنگاه نشان دهید که

$$g_1(x) = \prod_{\tau \in G} (x - \sum_i u_{\tau\sigma(i)}y_i).$$

نشان دهید این ایجاب می‌کند که $\deg g_i(x) = |G|$.

(ت) اگر $K = \mathbf{Q}$ ، $f \in \mathbf{Z}[x]$ تکین ، و p اول باشد ، $\bar{f} \in Z_p[x]$ را چندجمله‌ایی بگیرید که از f با تحویل ضرایب $f \pmod p$ به دست می‌آید . فرض کنید $\bar{f}$ در میدان‌تجزیه‌گر $\bar{F}$ روی Z_p دارای ریشه‌های متمایز $\bar{u}_1, \ldots, \bar{u}_n$ باشد . نشان دهیدکه

$$\bar{g}(x) = \prod_{\tau \in S_n} (x - \sum_i \bar{u}_i y_{\tau(i)}) \in \bar{F}[x, y_1, \ldots, y_n].$$

هرگاه $\bar{u}_i$ هاترتیب مناسب بیابند ، آنگاه ثابت کنید گروه گالوای $\bar{G}$ از $\bar{f}$ زیرگروهی‌از گروه گالوای G از f می‌باشد .

(ث) نشان دهید که $x^6 + 22x^5 - 9x^4 + 12x^3 - 37x^2 - 29x - 15 \in \mathbf{Q}[x]$ دارای گروه‌گالوای S_6 است . [**راهنمایی** . قسمت (ت) را با $p = 2, 3, 5$ به کار برید .]

(ج) گروه گالوای $x^5 - x - 1 \in \mathbf{Q}[x]$ مساوی S_5 است .

۱۴ . در اینجا روشی برای ساختن چند جمله‌ای $f \in \mathbf{Q}[x]$ با گروه گالوای S_n ، به‌ازای $n > 3$ ، ارائه می‌شود . این بستگی به وجود چندجمله‌ایهای تحویل‌ناپذیر از هر درجه در $Z_p[x]$ دارد (p اول است ؛ نتیجهٔ ۹.۵ زیر) . ابتدا $f_1, f_2, f_3 \in \mathbf{Z}[x]$ را طوری اختیار کنید که

(یک) $\deg f_i = n$ و $\bar{f}_i \in Z_2[x]$ تحویل‌ناپذیر باشد (نمادها مثل ۱۳ (ت)) ؛

(دو) $\deg f_2 = n$ و $\bar{f}_2 \in Z_3[x]$ در $Z_3[x]$ به صورت gh تجزیه شود، که در آن g تحویل‌ناپذیر و از درجهٔ $n-1$ بوده و h خطی باشد؛

(سه) $\deg f_3 = n$ و $f_3 \in Z_5[x]$ به صورت gh یا gh_1h_2 تجزیه شود، که در آنها g یک درجهٔ دوم تحویل‌ناپذیر در $Z_5[x]$ بوده و h, h_1, h_2 چند جمله‌ایهای تحویل‌ناپذیری از درجهٔ فرد در $Z_5[x]$ باشند.

(آ) فرض کنید $f = -15f_1 + 10f_2 + 6f_3$. در این صورت، $f \equiv f_1 \pmod 2$، $f \equiv f_2 \pmod 3$، و $f \equiv f_3 \pmod 5$.

(ب) گروه گالوای f یعنی G متعدی است (زیرا $\bar{f}$ در $Z_2[x]$ تحویل‌ناپذیر است).

(پ) G شامل یک دور از نوع $\sigma\lambda = \zeta = (i_1 i_2 \cdots i_{n-1})$ و عنصر σ است، که در آن σ یک ترانهش بوده و λ حاصلضربی از دورهـا از مرتبهٔ فرد است. بنابراین، $\sigma \in G$، که از آنجـا، بنـابر تمرین I ۳۰۶۰ و تعـدی، به‌ازای k ای $(1 \le k \le n-1)$، $(i_k i_n) \in G$.

(ت) $G = S_n$ (ر.ک. قسمت (پ) و تمرین I ۴۰۶۰ (ب)).

۵ میدانهای متناهی

در این بخش، میـدانهای متنـاهی (کـه گاهی *میدانهای گالوا* خوانده می‌شوند) کاملا" برحسب میدانهای تجزیه‌گر و ساختارآنها مشخص می‌گردند. نشان می‌دهیم که گروه گالوای یک توسیع یک میدان متناهی به وسیلهٔ یک میدان متناهی دوری است و مولد آن را صریحا" عرضه می‌کنیم.

با دو قضیه و یک لم شروع می‌کنیم که در میدانهایی به کار می‌روند که لزوما" متناهی **نیستند**. البته، درهرحالت، ما عمدتا" به نتایج مربوط به میدانهای متناهی علاقه‌مندیم.

قضیهٔ ۱۰۵. *فرض کنیم F یک میدان بوده و P اشتراک تمام زیرمیدانهای F باشد. در این صورت، P یک میدان بدون زیرمیدان حقیقی است. هرگاه (اول) $\mathrm{char}\, F = p$، آنگاه $P \cong Z_p$. هرگاه $\mathrm{char}\, F = 0$، آنگاه (میدان اعداد گویا) $P \cong Q$.*

میدان P *زیرمیدان اول* F نام دارد.

طرح برهان ۱۰۵. توجه کنیـد کـه هر زیر میدان F باید شامل 0 و 1_F باشد. فورا"

نتیجه‌می‌شود که P میدانی است که زیرمیدان حقیقی ندارد. واضح است که P شامل تمام عناصر به شکل $(m \in \mathbf{Z})\ m1_F$ می‌باشد. برای اتمام برهان می‌توان مستقیما" نشان دادکه اگر $\operatorname{char} F = p$ $P = \{m1_F \mid m \in \mathbf{Z}\}$ و اگر $\operatorname{char} F = 0$ $P = \{(m1_F)(n1_F)^{-1} \mid m,n \in \mathbf{Z}, n \neq 0\}$ یا اینکه بـه صورت زیر استدلال کرد. بنابر قضیهٔ III ۹۰۱۰، نگاشت $\varphi : \mathbf{Z} \to P$ داده شده با $m \mapsto m1_F$ یک همـریختی حلقـه‌ها با هستهٔ (n) است، که در آن $n = \operatorname{char} F$ و $n = 0$ یا n اول‌است. هرگاه $n = p$ (اول)، آنگاه $P \supset \operatorname{Im} \varphi \cong \mathbf{Z}/\operatorname{Ker} \varphi = \mathbf{Z}/(p) = Z_p$. چون Z_p میدان‌بوده و P زیرمیدان‌حقیقی ندارد، باید داشته باشیم $P = \operatorname{Im} \varphi \cong Z_p$. هرگاه $n = 0$، آنگاه $\varphi : \mathbf{Z} \to P$ تکریختی‌است‌و، بنابر نتیجهٔ III ۶.۴۰، یک تکریختی از میدانها مانند $\bar{\varphi} : \mathbf{Q} \to P$ وجوددارد. مثل قبل، باید داشته باشیم $P = \operatorname{Im} \bar{\varphi} \cong \mathbf{Q}$.

نتیجهٔ ۲۰۵. هرگاه F یک میدان متناهی باشد، آنگاه به‌ازای عدد اولی چون p و عدد صحیحی مانند $n \geq 1$ داریم $|F| = p^n$ و $\operatorname{char} F = p \neq 0$.

برهان. قضیهٔ III ۹۰۱۰ و قضیهٔ ۱۰۵ ایجاب می‌کنند که F دارای مشخص اول $p \neq 0$ اسـت. چـون F یک فضـای برداری با بعد متناهی روی زیرمیدان اول خود Z_p است، بنابر قضیهٔ IV ۴۰۲۰ (n جمعوند) $F \cong Z_p \oplus \cdots \oplus Z_p$؛ و در نتیجه، $|F| = p^n$.

در آینده زیرمیدان اول میدان F با مشخص p همیشه تحت یدریختی قضیهٔ ۱۰۵ با Z_p یکی‌گرفته می‌شود. مثلا"، خواهیم نوشت $Z_p \subset F$؛ بخصوص، 1_F با $1 \in Z_p$ یکی می‌شود.

قضیهٔ ۳۰۵. هرگاه F میدان‌و G زیرگروهی‌متناهی‌ازگروه‌ضربی عناصر ناصفر F باشد، آنگاه G یک‌گروه دوری‌است. بخصوص، گروه ضربی تمام عناصر ناصفر یک میدان متناهی دوری است.

برهان. اگر $G (\neq 1)$ یک گروه‌آبلی متناهی باشد، $G \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_k}$، که در آن، بنابر قضیهٔ II ۱۰۲۰، $m_1 > 1$ و $m_1 \mid m_2 \mid \cdots \mid m_k$. چون $m_k(\sum Z_{m_i}) = 0$، نتیجه می‌شود کـه هـر $u \in G$ ریشه‌ای از چندجمله‌ای $x^{m_k} - 1_F \in F[x]$ است (G یک گروه ضربی

است) . چون این چندجمله‌ای حداکثر m_k ریشهٔ متمایز در F دارد (قضیهٔ III ۷.۶۰) ، باید داشته باشیم $k = 1$ و $G \cong Z_{m_k}$.

نتیجهٔ ۴.۵ . *هرگاه F یک میدان متناهی باشد ، آنگاه F یک توسیع سادهٔ زیرمیدان اول‌خود Z_p است ؛ یعنی ، به‌ازای $u \in F$ ای ، $F = Z_p(u)$.*

طرح برهان . فرض کنید u یک مولد گروه ضربی عناصر ناصفر F باشد .

لم ۵.۵ . *هرگاه F میدانی با مشخص p بوده و $r \geq 1$ عددی صحیح باشد ، آنگاه نگاشت $\varphi : F \to F$ داده شده با $u \mapsto u^{p^r}$ یک Z_p ـ تکریختی میدانهاست . هرگاه F متناهی باشد ، آنگاه φ یک Z_p ـ خودریختی F است .*

طرح برهان . نکتهٔ مهم این است که ، برای مشخص p ، به‌ازای هر $u,v \in F$ ، $(u \pm v)^{p^r} = u^{p^r} \pm v^{p^r}$ (تمرین III ۱۱.۱۰) . چون $1_F \mapsto 1_F$ ، φ هر عنصر در زیرمیدان اول Z_p از F را ثابت می‌گذارد .

حال می‌توان توصیف مفیدی از میدانهای متناهی را ارائه داد .

حکم ۶.۵ . *فرض کنیم p اول و $n \geq 1$ عددی صحیح باشد . در این صورت ، F یک میدان متناهی با p^n عنصر است اگر و فقط اگر F یک میدان تجزیه‌گر $x^{p^n} - x$ روی Z_p باشد .*

برهان . هرگاه $|F| = p^n$ ، آنگاه گروه ضربی عناصر ناصفر F از مرتبهٔ $p^n - 1$ بوده ؛ و درنتیجه ، هر عنصر ناصفر $u \in F$ در $u^{p^n-1} = 1_F$ صدق می‌کند . لذا ، هر عنصر ناصفر $u \in F$ ریشه‌ای از $x^{p^n-1} - 1_F$ است ؛ ودرنتیجه ، ریشه‌ای از $x(x^{p^n-1} - 1_F) = x^{p^n} - x \in Z_p[x]$ نیز هست . چون $0 \in F$ ریشه‌ای از $x^{p^n} - x$ نیز هست ، $x^{p^n} - x$ دارای p^n ریشهٔ متمایز در F است (یعنی ، بنابر قضیهٔ III ۷.۶۰ ، روی F تجزیه می‌شود) و این ریشه‌ها دقیقاً " عناصر F می‌باشند . بنابراین ، F یک میدان‌تجزیه‌گر $x^{p^n} - x$ روی Z_p می‌باشد .

هرگاه F یک میدان تجزیه‌گر $f = x^{p^n} - x$ روی Z_p باشد، آنگاه، چون $\operatorname{char} F = \operatorname{char} Z_p = p$، $f' = -1$ و f نسبت به f' اول می‌باشند. بنابراین، طبق قضیهٔ III ۱۰.۶۰ (دو)، f دارای p^n ریشهٔ متمایز در F است. اگر φ تکریختی لم ۵.۵ (به‌ازای $r = n$) باشد، به‌آسانی معلوم می‌شود که $u \in F$ ریشه‌ای از f است اگر و فقط اگر $\varphi(u) = u$. با استفاده از این تحقیق کنید که مجموعهٔ E مرکب از تمام ریشه‌های f در F زیرمیدانی از F ازمرتبهٔ p^n است، که‌لزوما "شامل‌زیرمیدان‌اول Z_p از F می‌باشد. چون F یک میدان تجزیه‌گر است، روی Z_p به وسیلهٔ ریشه‌های f (یعنی، عناصر E) تولید می‌شود. بنابراین، $F = Z_p(E) = E$.

نتیجهٔ ۷.۵. هرگاه p اول بوده و $n \geq 1$ عدد صحیحی باشد، آنگاه میدانی با p^n عنصر وجود دارد. هر دو میدان متناهی با تعداد عناصر یکسان یکریخت‌اند.

برهان. به‌ازای p و n داده شده، طبق قضیهٔ ۲.۳، یک میدان تجزیه‌گر مانند F از $x^{p^n} - x$ روی Z_p وجود دارد و، بنابر حکم ۶.۵، از مرتبهٔ p^n است. چون بنابر حکم ۶.۵ هر میدان متناهی از مرتبهٔ p^n یک میدان تجزیه‌گر $x^{p^n} - x$ روی Z_p است، پس طبق نتیجهٔ ۹.۳ هر دو میدان از این نوع یکریخت‌اند.

نتیجهٔ ۸.۵. هرگاه K میدانی متناهی بوده و $n \geq 1$ عددی صحیح باشد، آنگاه یک توسیع میدان ساده مانند $F = K(u)$ از K وجود دارد به‌طوری‌که F متناهی بوده و $[F : K] = n$. هر دو توسیع میدان n بعدی از K، K ـ یکریخت‌اند.

طرح برهان. اگر K از مرتبهٔ p^r باشد، F را یک میدان تجزیه‌گر $f = x^{p^{rn}} - x$ روی K می‌گیریم. بنابرحکم ۶.۵، هر $u \in K$ در $u^{p^r} = u$ صدق می‌کند و به استقرا معلوم می‌شود که، به‌ازای هر $u \in K$، $u^{p^{rn}} = u$. بنابراین، F عملا" یک میدان تجزیه‌گر f روی Z_p است (تمرین ۳.۳). برهان حکم ۶.۵ نشان می‌دهد که F درست از p^{nr} ریشهٔ متمایز f تشکیل شده است. لذا، $p^{nr} = |F| = |K|^{[F:K]} = (p^r)^{[F:K]}$، که از آنجا $[F : K] = n$. نتیجهٔ ۴.۵ ایجاب می‌کند که F یک توسیع سادهٔ K می‌باشد. هرگاه F_1 توسیع میدان دیگری از K با خاصیت $[F_1 : K] = n$ باشد، آنگاه $[F_1 : Z_p] = n[K : Z_p] = nr$، که از آنجا

$|F_1| = p^{nr}$. بنابر حکم ۶.۵ ، F_1 یک میدان تجزیه‌گر $x^{p^{nr}} - x$ روی Z_p ، و درنتیجه روی K ، است. لذا، طبق نتیجهٔ ۹.۳ ، F و F_1 ، K ـ یکریخت می‌باشند .

نتیجهٔ ۹.۵ . هرگاه K میدانی متناهی بوده و $n \geq 1$ عددی صحیح باشد ، آنگاه یک چندجمله‌ای تحویل‌ناپذیر از درجهٔ n در K[x] وجود خواهد داشت .

برهان . تمرین ؛ از نتیجهٔ ۸.۵ و قضیهٔ ۶.۱ استفاده کنید .

حکم ۱۰.۵ . هرگاه F یک‌توسیع میدان‌با بعد متناهی از میدان متناهی K باشد ، آنگاه F متناهی بوده و روی K گالوا می‌باشد . گروه گالوای $Aut_K F$ دوری است .

طرح برهان . فرض کنیم Z_p زیرمیدان‌اول K باشد . در این صورت ، F روی Z_p با بعد متناهی است (قضیهٔ ۲.۱) ؛ مثلا " ، با بعد n است ، که ایجاب می‌کند که $|F| = p^n$. بنابر برهان حکم ۶.۵ و تمرین ۲.۳ ، F یک میدان تجزیه‌گر روی Z_p ، و درنتیجه روی K ، از $x^{p^n} - x$ است که تمام ریشه‌هایش متمایزند . قضیهٔ ۱۱.۳ ایجاب می‌کند که F روی K گالوا باشد. بنابر لم ۵.۵ ، نگاشت $\varphi : F \to F$ داده شده با $u \mapsto u^p$ یک Z_p ـ خودریختی است . واضح است که φ^n همانی بوده، و هیچ توان پایین‌تر k از φ نمی‌تواند همانی باشد (زیرا این ایجاب می‌کند که $x^{p^k} - x$ ، p^n ریشهٔ متمایز در F داشته باشد و $k < n$ ، که با قضیهٔ III ۷.۶۰ تعارض دارد) . چون بنابر قضیهٔ اساسی $|\mathrm{Aut}_{Z_p} F| = n$ ، $\mathrm{Aut}_{Z_p} F$ باید گروه دوری تولید شده به وسیلهٔ φ باشد . چون $\mathrm{Aut}_K F$ زیرگروهی از $\mathrm{Aut}_{Z_p} F$ است ، بنابر قضیهٔ I ۵.۳۰ ، $\mathrm{Aut}_K F$ دوری می‌باشد .

تمرینات

تذکر. F همواره یک توسیع میدان از یک میدان K است .

۱ . اگر K یک میدان‌متناهی‌با مشخص p باشد ، ساختار گروه جمعی K را توصیف کنید .

۲ . (فرما) هرگاه $p \in \mathbf{Z}$ اول باشد ، آنگاه به‌ازای هر $a \in Z_p$ ، $a^p = a$ یا ، معادلا " ، به‌ازای هر $c \in \mathbf{Z}$ ، $c^p \equiv c \pmod p$.

۳ . هرگاه $|K| = p^n$ ، آنگاه‌هرعنصر K دارای‌ریشهٔ p ام منحصر به فردی در K است .

۴ . هرگاه ریشه‌های چندجمله‌ای تکین $f \in K[x]$ (در میدان تجزیه‌گری از f روی K) متمایز بوده و میدان تشکیل دهند، آنگاه $\operatorname{char} K = p$ و، به‌ازای $n \geq 1$ ی، $f = x^{p^n} - x$.

۵ . (آ) میدانی با 9 عنصر ساخته و جداول جمع و ضرب آن را بنویسید.
(ب) همین‌کار را برای یک میدان با 25 عنصر انجام دهید.

۶ . هرگاه $|K| = q$ و $(n,q) = 1$ و F یک میدان تجزیه‌گر $x^n - 1_K$ روی K باشد، آنگاه $n \mid (q^k - 1)$ کوچکترین عدد صحیح مثبت k است که $[F : K]$.

۷ . هرگاه $|K| = q$ و $f \in K[x]$ تحویل‌ناپذیر باشد، آنگاه f ، $x^{q^n} - x$ را عاد می‌کند اگر و فقط اگر $\deg f$ ، n را عاد کند.

۸ . هرگاه $|K| = p^r$ و $|F| = p^n$ ، آنگاه $r \mid n$ و $\operatorname{Aut}_K F$ دوری با مولد φ است که با $u \mapsto u^{p^r}$ داده می‌شود.

۹ . هرگاه $n \geq 3$ ، آنگاه $x^{2^n} + x + 1$ روی Z_2 تحویل‌پذیر است.

۱۰ . هر عنصر در یک میدان متناهی را می‌توان به صورت مجموعی از دو مربع نوشت.

۱۱ . فرض کنید F یک بست جبری Z_p (p اول) باشد.
(آ) F روی Z_p گالوای جبری است.
(ب) نگاشت $\varphi : F \to F$ داده‌شده با $u \mapsto u^p$ یک Z_p ـ خودریختی غیرهمانی F است.
(پ) زیرگروه $H = \langle \varphi \rangle$ یک زیرگروه حقیقی $\operatorname{Aut}_{Z_p} F$ است که میدان ثابت آن Z_p است که بنابر (آ)، میدان ثابت $\operatorname{Aut}_{Z_p} F$ نیز می‌باشد.

۱۲ . هرگاه K متناهی بوده و F یک بست جبری K باشد، آنگاه $\operatorname{Aut}_K F$ آبلی است. هر عنصر $\operatorname{Aut}_K F$ (جز 1_F) از مرتبهٔ نامتناهی می‌باشد.

۶ جدایی‌پذیری

بررسی جدایی‌پذیری با توجه به مفهومی که، از یک جهت، کاملا " مقابل جدایی‌پذیری است به نحو چشمگیری ساده می‌شود. درنتیجه، بخش را صرفا " با توسیعهای جدایی‌ناپذیر، که در قضیهٔ ۴.۶ به طرق مختلف توصیف می‌شوند، آغاز می‌کنیم. سپس با استفاده از این ایده‌ها تمام مطالب مهم در باب جدایی‌پذیری توسیعهای جبری (اصولا " قضیهٔ ۷.۶) را ثابت می‌کنیم. درجهٔ جدایی (نا)پذیری یک توسیع جبری را به تفصیل مطرح می‌کنیم (اما اغلب این مطالب در آینده لازم نیستند). بالاخره، قضیهٔ عنصر اولیه را ثابت

می‌کنیم (حکم ۱۵۰۶) . این نتیجه از بقیهٔ بخش مستقل بوده و می‌توان آن‌رادر هر زمان خواند .

تعریف ۱۰۶ . فرض‌کنیم F یک‌توسیع میدان K باشد . عنصرجبری $u \in F$ روی K ***صرفا " جدایی‌ناپذیر*** است اگر چندجمله‌ای تحویل‌ناپذیر f مربوط به‌آن از $K[x]$ در $F[x]$ به صورت $f = (x - u)^m$ تجزیه‌شود . F یک‌***توسیع صرفا "جدایی‌ناپذیر*** K است اگر هر عنصر F روی K صرفا " جدایی‌ناپذیر باشد .

لذا ، u روی K جدایی‌پذیراست اگرچندجمله‌ای تحویل‌ناپذیر f از درجهٔ n آن دارای n ریشهٔ متمایز (در میدان تجزیه‌گری) بوده و روی K صرفا " جدایی‌ناپذیر است اگر f دقیقا " یک ریشه داشته باشد . ممکن است عنصری داشته باشیم که نه روی K جدایی‌پذیر باشد نه‌صرفا " جدایی‌ناپذیر .

قضیهٔ ۲۰۶ . فرض‌کنیم F یک توسیع میدان K باشد . در این صورت ، $u \in F$ روی K جدایی‌پذیر و صرفا " جدایی‌ناپذیر است اگر و فقط‌اگر $u \in K$.

برهان . عنصر $u \in F$ روی K جدایی‌پذیر و صرفا " جدایی‌ناپذیر است اگر و فقط‌اگر چندجمله‌ای تحویل‌ناپذیر آن به شکل $(x - u)^m$ بوده و در میدان تجزیه‌گری m ریشهٔ متمایز داشته باشد . واضح است که این فقط‌وقتی رخ می‌دهد که $m = 1$ ؛ درنتیجه ، $x - u \in K[x]$ و $u \in K$.

هرگاه $\text{char } K = 0$ ، آنگاه هر عنصر جبری روی K جدایی‌پذیر روی K است . بنابراین ،قضیهٔ ۲۰۶ ایجاب می‌کند که تنها عنصرهایی که روی K صرفا " جدایی‌ناپذیرند عناصرخود K هستند .لذا ،توسیعهای‌صرفا "جدایی‌ناپذیر K بدیهی‌اند‌اگر $\text{char } K = 0$. درنتیجه ، معمولا " توجه ما معطوف مشخص (اول) ناصفر می‌گردد . ما بارها از این امر در باب مشخص p بدون ذکر صریح آن استفاده خواهیم کرد : هرگاه $\text{char } K = p \neq 0$ و $u, v \in K$ ، آنگاه ، به‌ازای هر $n \geq 0$ ، $(u \pm v)^{p^n} = u^{p^n} \pm v^{p^n}$ (تمرین III ۱۱۰۱۰) . برای توصیف توسیعهای صرفا " جدایی‌ناپذیر ، لم زیر مورد نیاز است .

لم ۳۰۶. *فرض کنیم F یک توسیع میدان K با خاصیت $\mathrm{char}\, K = p \neq 0$ باشد. هرگاه $u \in F$ روی K جبری باشد، آنگاه، به‌ازای $n \geq 0$ ی، u^{p^n} روی K جدایی‌پذیر است.*

طرح برهان. از استقرا بر درجهٔ u روی K استفاده می‌کنیم. اگر $\deg u = 1$ یا u جدایی‌پذیر باشد، لم برقرار است. هرگاه f چندجمله‌ای تحویل‌ناپذیر از u ی جدایی‌ناپذیر با درجهٔ بزرگتر از یک باشد، آنگاه $f' = 0$ (قضیهٔ III، ۱۰۰۶) ، که از آنجا f یک چندجمله‌ای از x^p می‌باشد (تمرین III ۳۰۶۰). بنابراین، u^p روی K جبری از درجهٔ کوچکتر از $\deg u$ است، که از آنجا، بنابر استقرا، $(u^p)^{p^m}$ به‌ازای $m \geq 0$ ی روی K جدایی‌پذیر است.

قضیهٔ ۴۰۶. *هرگاه F یک توسیع میدان جبری میدان K با مشخص $p \neq 0$ باشد، آنگاه احکام زیر باهم معادلند:*

(یک) F روی K صرفا "جدایی‌ناپذیر است؛

(دو) چندجمله‌ای تحویل‌ناپذیر مربوط به هر $u \in F$ به شکل $x^{p^n} - a \in K[x]$ است؛

(سه) هرگاه $u \in F$، آنگاه، به‌ازای $n \geq 0$ ی، $u^{p^n} \in K$؛

(چهار) تنها عنصرهایی از F که روی K جدایی‌پذیرند عناصر خود K می‌باشند؛

(پنج) F روی K با مجموعهٔ عناصر صرفا "جدایی‌ناپذیر تولید می‌شود.

طرح برهان. (دو) $\Rightarrow$ (یک) فرض کنیم $(x-u)^m$ چندجمله‌ای تحویل‌ناپذیر از $u \in F$ بوده و $m = np^r$، که در آن $(n,p) = 1$. پس، بنابر تمرین III ۱۱۰۱۰، $(x-u)^m = (x-u)^{p^r n} = (x^{p^r} - u^{p^r})^n$، چون $(x-u)^m \in K[x]$. ضریب $x^{p^r(n-1)}$، یعنی $\pm nu^{p^r}$ (قضیهٔ III ۶۰۱۰)، باید در K باشد. اما $(p,n) = 1$ ایجاب می‌کند که $u^{p^r} \in K$ (تمرین ۱). چون $(x-u)^m = (x^{p^r} - u^{p^r})^n$ در $K[x]$ تحویل‌ناپذیر است، باید داشته باشیم $n = 1$ و $(x-u)^m = x^{p^r} - a$، که در آن $a = u^{p^r} \in K$.

استلزامهای (سه) $\Rightarrow$ (دو) و (پنج) $\Rightarrow$ (یک) بدیهی‌اند. بنابر تمرین III ۱۱۰۱۰ (یک) $\Rightarrow$ (سه)؛ بنابر قضیهٔ ۲۰۶، (چهار) $\Rightarrow$ (یک)؛ و بنابر لم ۳۰۶، (سه) $\Rightarrow$ (چهار) $\Rightarrow$ (سه) هرگاه u روی K صرفا "جدایی‌ناپذیر باشد، آنگاه برهان (دو) $\Rightarrow$ (یک) نشان می‌دهد که به‌ازای $n \geq 0$ ی: $u^{p^n} \in K$. اگر $u \in F$ دلخواه باشد،

از قضیهٔ ۳۰۱ و تمرین III ۱۱۰۱۰ استفاده کنید.

نتیجهٔ ۵۰۶. *هرگاه* F *یک توسیع میدان صرفاً "جدایی‌ناپذیر با بعد متناهی بوده و* $char\ K = p \neq 0$ *، آنگاه، به‌ازای* $n \geq 0$ *ی،* $[F:K] = p^n$.

برهان. بنابر قضیهٔ ۱۱۰۱، $F = K(u_1, \ldots, u_m)$. طبق فرض، هر u_i روی K، و درنتیجه روی $K(u_1, \ldots, u_{i-1})$، صرفاً "جدایی‌ناپذیر است" (تمرین ۲) قضایای ۶۰۱ و ۴۰۶ (دو) ایجاب می‌کنند که هر مرحله از زنجیر $K \subset K(u_1) \subset K(u_1,u_2) \subset \cdots \subset K(u_1, \ldots, u_m) = F$ بعدی دارد که توانی از p است. بنابراین، طبق قضیهٔ ۲۰۱، $[F:K] = p^n$.

برای قضیهٔ اصلی در باب جدایی‌پذیری، لم دیگری نیز مورد نیاز است.

لم ۶۰۶. *هرگاه* F *یک توسیع میدان* K *بوده،* X *زیرمجموعه‌ای از* F *باشد که* $F = K(X)$ *، و هر عنصر* X *روی* K *جدایی‌پذیر باشد، آنگاه* F *یک توسیع جدایی‌پذیر از* K *می‌باشد.*

برهان. هرگاه $v \in F$ ، آنگاه، طبق قضیهٔ ۳۰۱، عناصری چون $u_1, \ldots, u_n \in X$ وجود دارند به‌طوری‌که $v \in K(u_1, \ldots, u_n)$. فرض کنیم $f_i \in K[x]$ چندجمله‌ای جدایی‌پذیر تحویل‌ناپذیر از u_i بوده و E یک میدان تجزیه‌گر $\{f_1, \ldots, f_n\}$ روی $K(u_1, \ldots, u_n)$ باشد. در این صورت، E یک میدان تجزیه‌گر $\{f_1, \ldots, f_n\}$ روی K نیز هست (تمرین ۳۰۳). بنابر قضیهٔ ۱۱۰۳، E روی K جدایی‌پذیر (درواقع، گالوا) است، که ایجاب می‌کندکه $v \in K(u_1, \ldots, u_n) \subset E$ روی K جدایی‌پذیر باشد.

قضیهٔ ۷۰۶. *فرض کنیم* F *یک توسیع میدان جبری از* K *بوده،* S *مجموعهٔ تمام عناصر* F *باشد که روی* K *جدایی‌پذیرند، و* P *مجموعهٔ تمام عناصری از* F *باشد که روی* K *صرفاً "جدایی‌ناپذیرند".*

(یک) S *یک توسیع میدان جدایی‌پذیر* K *است.*

(دو) F *روی* S *صرفاً "جدایی‌ناپذیر است.*

(سه) P یک توسیع میدان صرفا " جدایی‌ناپذیر K است .

(چهار) $P \cap S = K$.

(پنج) F روی P جدایی‌پذیر است اگر و فقط اگر $F = SP$.

(شش) هرگاه F روی K نرمال باشد ، آنگاه S روی K گالوا است ، F روی P گالوا است ، و $Aut_K S \cong Aut_P F = Aut_K F$.

چند تبصره. واضح است که S بزرگترین زیرمیدان منحصر به فرد F است که روی K جدایی‌پذیر است و S شامل هر میدان میانی جدایی‌پذیر روی K است ؛ به همین نحو ، در مورد P و میدانهای میانی صرفا " جدایی‌ناپذیر . هرگاه $\text{char } K = 0$ ، آنگاه $S = F$ و $P = K$ (قضیهٔ ۲۰۶) .

طرح برهان ۷۰۶ .(یک)هرگاه $u, v \in S$ و $v \neq 0$ ، آنگاه ، طبق لم ۶۰۶ ، $K(u,v)$ روی K جدایی‌پذیر است ، که ایجاب می‌کند که $u - v, uv^{-1} \in S$. بنابراین ، S یک زیرمیدان است . لم ۳۰۶ و قضیهٔ ۴۰۶ قسمت (دو) را ایجاب می‌کنند . قسمت (سه) تمرینی عادی است که با استفاده از تمرین III ۱۱۰۱۰ اگر $\text{char } K = p$ و اینکه $P = K$ اگر $\text{char } K = 0$ به دست می‌آید . قضیهٔ ۲۰۶ قسمت (چهار) را ایجاب می‌کند .

(پنج) هرگاه $\bar{F}$ روی P جدایی‌پذیر باشد ، آنگاه $\bar{F}$ روی میدان مرکب $\overline{SP}$ جدایی‌پذیر است (تمرین ۱۲۰۳) و روی SP صرفا " جدایی‌ناپذیر است (قسمت (دو) و تمرین ۲) . بنابراین ، طبق قضیهٔ ۲۰۶ ، $\bar{F} = \overline{SP}$. به عکس ، هرگاه $F = \overline{SP} = P(S)$ ، آنگاه ، طبق تمرین ۱۲،۳ و لم ۶۰۶ ، F روی $\bar{P}$ جدایی‌پذیر است .

(شش) ابتدانشان‌می‌دهیم‌که‌میدان‌ثابت K_0 از $\text{Aut}_K F$ عملا " P است ، که فورا " ایجاب می‌کند که F روی P گالوا است و $\text{Aut}_P F = \text{Aut}_K F$. فرض‌کنیم $u \in F$ دارای چندجمله‌ای تحویل‌ناپذیر f روی K بوده و همچنین $\sigma \in \text{Aut}_K F$ ؛ $\sigma(u)$ ریشه‌ای‌از f است (قضیهٔ ۲۰۲) . هرگاه $u \in P$ ، آنگاه $f = (x-u)^m$ ؛ و درنتیجه ، $\sigma(u) = u$. بنابراین ، $P \subset K_0$. هرگاه $u \in K_0$ و $v \in F$ ریشهٔ‌دیگری از f باشد ، آنگاه یک K ــ یکریختی مانند $\tau : K(u) \to K(v)$ وجود دارد به‌طوری‌که $\tau(u) = v$ (نتیجهٔ ۹۰۱) . بنابر قضایای ۸۰۳ و ۱۴۰۳ و تمرین ۲۰۳ ، τ به یک K ــ خودریختی مانند F توسیع می‌یابد . چون $u \in K_0$ ، داریم $u = \tau(u) = v$. چون بنابرنرمالی f در $F[x]$ تجزیه می‌شود ، این استدلال نشان

می‌دهد که به‌ازای m ی $f = (x-u)^m$. بنابراین، $u \in P$ و $P \supset K_0$.ازاینرو، $P = K_0$.

هر $\sigma \in \mathrm{Aut}_P F = \mathrm{Aut}_K F$ باید عناصر جدایی‌پذیر را به عناصر جدایی‌پذیر ببرد (قضیهٔ ۲۰۲) . بنابراین، انتساب $\sigma \mapsto \sigma | S$ یک همریختی مانند $\theta : \mathrm{Aut}_P F \to \mathrm{Aut}_K S$ را تعریف می‌کند. چون F روی S نرمال است، θ برووریختی می‌باشد (قضایای ۸۰۳ و ۱۴۰۳ و تمرین ۲۰۳) . چون F روی P گالواست، بنابر (پنج) $F = SP$ ، که ایجاب می‌کندکه θ یک تکریختی است. از اینرو، $\mathrm{Aut}_P F \cong \mathrm{Aut}_K S$. بالاخره، فرض کنیم $u \in S$ به وسیلهٔ تمام $\sigma \in \mathrm{Aut}_K S$ های شابت نگه داشته شود. چون θ برووریختی است، u در میدان شابت P از $\mathrm{Aut}_P F$ است، که از آنجا $u \in P \cap S = K$. بنابراین، S روی K گالوا می‌باشد.

نتیجهٔ ۸۰۶ . هرگاه F یک توسیع میدان جدایی‌پذیر E بوده و E یک توسیع میدان جدایی‌پذیر K باشد، آنگاه F روی K جدایی‌پذیر است.

برهان. هرگاه S همانند در قضیهٔ ۷۰۶ باشد، آنگاه $E \subset S$ و F روی S صرفا " جدایی‌ناپذیر است. اما F روی E ، و درنتیجه روی S ، جدایی‌پذیر است (تمرین ۱۲۰۳) . بنابراین، طبق قضیهٔ ۲۰۶ ، $F = S$.

فرض کنیم F یک میدان با مشخص $p \neq 0$ باشد. لم ۵۰۵ نشان می‌دهد که به‌ازای هر $n \geq 1$ ، مجموعهٔ $F^{p^n} = \{u^{p^n} \mid u \in F\}$ زیرمیدانی‌از F است. بنابرقضیهٔ ۴۰۶ (سه) ، F روی F^{p^n} ، و درنتیجه روی هر میدان میانی، صرفا " جدایی‌ناپذیر است (تمرین ۲) .

نتیجهٔ ۹۰۶ . فرض کنیم F یک توسیع میدان جبری از K با خاصیت $\mathrm{char}\, K = p \neq 0$ باشد. هرگاه F روی K جدایی‌پذیر باشد، آنگاه، به‌ازای هر $n \geq 1$ ، $F = KF^{p^n}$. هرگاه $[F : K]$ متناهی بوده و $F = KF^p$ ، آنگاه F روی K جدایی‌پذیر است. بخصوص، $u \in F$ روی K جدایی‌پذیر است اگر و فقط اگر $K(u^p) = K(u)$.

طرح برهان. فرض کنیم S همانند در قضیهٔ ۷۰۶ باشد. هرگاه $[F : K]$ متناهی باشد، آنگاه، بنابر قضیهٔ ۱۱۰۱ ، $F = K(u_1, \ldots, u_m) = S(u_1, \ldots, u_m)$. چون هر u_i روی S

صرفا" جدایی‌ناپذیر است (قضیهٔ ۷۰۶)، $n \geq 1$ ی هست به‌طوری‌که به‌ازای هر i، $u_i^{p^n} \in S$. چون $F = S(u_1, \ldots, u_m)$، تمرین III ۱۱۰۱۰ و قضیهٔ ۳۰۱ ایجاب می‌کنند که $F^{p^n} \subset S$. واضح است که هر عنصر S روی F^{p^n}، و درنتیجه روی KF^{p^n}، صرفا" جدایی‌ناپذیر است. S روی K، و درنتیجه روی KF^{p^n}، جدایی‌پذیر است. بنابراین، طبق قضیهٔ ۲۰۶، $S = KF^{p^n}$. با استفاده‌از $\text{char } K = p$ و قضیهٔ ۳۰۱، نشان دهید که به‌ازای هر $t \geq 1$، $F^{p^t} = [K(u_1, \ldots, u_m)]^{p^t} = K^{p^t}(u_1^{p^t}, \ldots, u_m^{p^t})$. درنتیجه، به‌ازای هر $t \geq 1$، داریم $KF^{p^t} = K(K^{p^t}(u_1^{p^t}, \ldots, u_m^{p^t}) = K(u_1^{p^t}, \ldots, u_m^{p^t})$. توجه کنید که این استدلال به‌ازای مولدهای **دلخواه** $u_1, \ldots, u_m$ از F روی K کار می‌کند. اما، هرگاه $F = KF^p$، آنگاه $K(u_1, \ldots, u_m) = F = KF^p = K(u_1^p, \ldots, u_m^p)$. استدلال مکرر با مولدهای $u_i^{p^t}$ به جای u_i $[i = 1, 2, \ldots, n]$ نشان می‌دهد که $F = K(u_1, \ldots, u_m) = K(u_1^{p^n}, \ldots, u_m^{p^n}) = KF^{p^n} = S$، که از آنجا F روی K جدایی‌پذیر است. به عکس، هرگاه F روی K جدایی‌پذیر باشد، آنگاه F روی KF^{p^n} (به‌ازای هر $n \geq 1$) جدایی‌پذیر و صرفا" جدایی‌ناپذیر است. بنابراین، طبق قضیهٔ ۲۰۶، $F = KF^{p^n}$.

حال جدایی‌پذیری و جدایی‌ناپذیری را ازدیدگاه‌متفاوتی درنظر می‌گیریم. با آنکه حکم ۱۲۰۶ در بخش ۷ به کار رفت، آنچه واقعا" برای درک مطالب آتی لازم است تعریف ۱۰۰۶ و تبصره‌های بعد از آن می‌باشند.

تعریف ۱۰۰۶. فرض کنیم F یک توسیع میدان جبری از K و S بزرگترین زیرمیدانی از F باشدکه‌روی K جدایی‌پذیر است (مثل قضیهٔ ۷۰۶). بعد $[S : K]$ **درجهٔ جدایی‌پذیر** F روی K نام دارد و با $[F : K]_s$ نموده می‌شود. بعد $[F : S]$ **درجهٔ جدایی‌ناپذیر** (یا **درجهٔ جدایی‌ناپذیری**) F روی K نام دارد و با $[F : K]_i$ نموده می‌شود.

چند تبصره. $[F : K]_s = [F : K]$ و $[F : K]_i = 1$ اگروفقط‌اگر F روی K جدایی‌پذیرباشد. $[F : K]_s = 1$ و $[F : K]_i = [F : K]$ اگر و فقط‌اگر F روی K صرفا "جدایی‌ناپذیر باشد. در هر حالت، بنابر قضیهٔ ۲۰۱، $[F : K] = [F : K]_s[F : K]_i$. هرگاه $[F : K]$ متناهی بوده و $\text{char } K = p \neq 0$، آنگاه، طبق نتیجهٔ ۵۰۶ و قضیهٔ ۷۰۶ (دو)، توانی از p $[F : K]_i$

می‌باشد . لم زیر به ما توان توصیف دیگری از $[F:K]_s$ و نشان دادن اینکه به‌ازای هر میدان میانی E ، $[F:K]_s = [F:E]_s[E:K]_s$ می‌بخشد .

لم ۱۱.۶ . *فرض کنیم F یک توسیع میدان E ، E یک توسیع میدان K ، و N یک توسیع میدان نرمال از K شامل F باشد . هرگاه r عدد اصلی E ـ تکریختیهای متمایز $F \to N$ و t عدد اصلی K ـ تکریختیهای $E \to N$ باشد ، آنگاه rt عدد اصلی K ـ تکریختیهای متمایز $F \to N$ می‌باشد .*

برهان . برای راحتی ، فرض کنیم r, t متناهی باشند . همین برهان با تعدیل مختصر نمادها در حالت کلی به کار می‌رود . فرض کنیم $\tau_1, \ldots, \tau_r$ تمام E ـ تکریختیهای $F \to N$ متمایز و $\sigma_1, \ldots, \sigma_t$ تمام K ـ تکریختیهای $E \to N$ متمایز باشند . هر σ_i به یک K ـ خودریختی N توسیع می‌یابد (قضایای ۸.۳ و ۱۴.۳ و تمرین ۲.۳) که این نیز با σ_i نموده می‌شود . هر نگاشت مرکب $\sigma_i\tau_j$ یک K ـ تکریختی مانند $F \to N$ است . هرگاه $\sigma_i\tau_j = \sigma_a\tau_b$ ، آنگاه $\sigma_a^{-1}\sigma_i\tau_j = \tau_b$ که ایجاب می‌کند که $\sigma_a^{-1}\sigma_i | E = 1_E$. درنتیجه ، داریم $\sigma_i = \sigma_a$ و $i = a$. چون σ_i انژکتیو است ، $\sigma_i\tau_j = \sigma_i\tau_b$ ایجاب می‌کند که $\tau_j = \tau_b$ و $j = b$. بنابراین ، rt ، K ـ تکریختی $\sigma_i\tau_j : F \to N$ $(1 \le i \le t, 1 \le j \le r)$ همه متمایز می‌باشند . فرض کنیم $\sigma : F \to N$ یک K ـ تکریختی باشد . پس به‌ازای i ی $\sigma | E = \sigma_i$ و $\sigma_i^{-1}\sigma$ یک $\overline{K}$ ـ تکریختی مانند $F \to N$ است ، که بر E همانی می‌باشد . بنابراین ، به‌ازای j ای ، $\sigma_i^{-1}\sigma = \tau_j$ ، که از آنجا $\sigma = \sigma_i\tau_j$. لذا ، rt نگاشت متمایز همهٔ K ـ تکریختی $F \to N$ می‌باشند .

حکم ۱۲.۶ . *فرض کنیم F یک توسیع میدان با بعد متناهی از K بوده و N یک توسیع میدان نرمال K شامل F باشد . تعداد K ـ تکریختیهای $F \to N$ دقیقاً " مساوی $[F:K]_s$ یعنی درجهٔ جدایی‌پذیر F روی K ، می‌باشد .*

طرح برهان . فرض کنیم S زیرمیدان ماکزیمال F جدایی‌پذیر روی K باشد (قضیهٔ ۷.۶ (یک)) . هر $\overline{K}$ ـ تکریختی $S \to N$ به یک K ـ خودریختی N (قضایای ۸.۳ و ۱۴.۳ و تمرین ۲.۳) ؛ و درنتیجه (با تحدید) ، به یک K ـ تکریختی $F \to N$ توسیع

می‌یابد. حکم می‌کنیم که تعداد K ـ تکریختیهای متمایز $F \to N$ همان تعداد K ـ تکریختیهای متمایز $N \to S$ است. این در حالت $\operatorname{char} K = 0$ بداهتاً درست است، زیرا در این حالت $F = S$. درنتیجه، فرض کنیم $\operatorname{char} K = p \neq 0$ و σ, τ، K ـ تکریختیهای $F \to N$ باشند به‌طوری‌که $\sigma | S = \tau | S$. هرگاه $u \in F$، آنگاه، بنابر قضایای ۴.۶ و ۷.۶ (دو)، به‌ازای $n \geq 0$ ی، $u^{p^n} \in S$. بنابراین،

$$\sigma(u)^{p^n} = \sigma(u^{p^n}) = \tau(u^{p^n}) = \tau(u)^{p^n},$$

که از آنجا $\sigma(u) = \tau(u)$. لذا، $\sigma | S = \tau | S$ ایجاب می‌کند که $\sigma = \tau$، که حکم ما را ثابت می‌کند. درنتیجه، کافی است فرض کنیم F روی K جدایی‌پذیر است (یعنی، $F = S$)، که در این حالت به‌ازای هر میدان میانی E داریم $[F : K] = [F : K]_s$، $[F : E] = [F : E]_s$، و $[E : K] = [E : K]_s$ (تمرین ۱۲.۳).

حال به استقرا بر $n = [F : K] = [F : K]_s$ عمل می‌کنیم؛ حالت $n = 1$ بدیهی است. اگر $n > 1$، $u \notin F - K$ را اختیار می‌کنیم؛ در این صورت، $[K(u) : K] = r > 1$. اگر $r < n$، از فرض استقرا و لم ۱۱.۶ (به‌ازای $E = K(u)$) استفاده کرده قضیه را ثابت می‌کنیم. هرگاه $r = n$، آنگاه $F = K(u)$ و $[F : K]$ درجهٔ چندجمله‌ای تحویل‌ناپذیر (جدایی‌پذیر) $f \in K[x]$ از u است. هر K ـ تکریختی $\sigma : F \to N$ کاملاً با $v = f(u)$ معین می‌شود. چون v ریشه‌ای از f (مثل قضیهٔ ۲.۲) است، حداکثر $[F : K] = \deg f$ از این K ـ تکریختیها وجود دارند. چون f بنابر نرمالی در N تجزیه می‌شود و جدایی‌پذیر است، نتیجهٔ ۹.۱ نشان می‌دهد که دقیقاً $[F : K]$ ، K ـ تکریختی متمایز $F \to N$ وجود دارند.

نتیجهٔ ۱۳.۶. *هرگاه F یک توسیع میدان E و E یک توسیع میدان K باشد، آنگاه*

$$[F : E]_i[E : K]_i = [F : K]_i \quad \text{و} \quad [F : E]_s[E : K]_s = [F : K]_s.$$

برهان. تمرین؛ از لم ۱۱.۶ و حکم ۱۲.۶ استفاده کنید.

نتیجهٔ ۱۴.۶. *فرض کنیم $f \in K[x]$ یک چندجمله‌ای تکین تحویل‌ناپذیر روی میدان K، F یک میدان تجزیه‌گر f روی K، و u_1 ریشه‌ای از f در F باشد. در این صورت،*
(یک) هر ریشهٔ f دارای بستایی $[K(u_1) : K]_i$ است؛ درنتیجه، در $F[x]$،

$$f = [(x - u_1)\cdots(x - u_n)]^{[K(u_1):K]_i},$$

که در آن $u_1, \ldots, u_n$ همه ریشه‌های متمایز f بوده و $n = [K(u_1) : K]_s$.

(دو) $u_1^{[K(u_1):K]_i}$ روی K جدایی‌پذیر است.

طرح برهان. فرض کنیم $\operatorname{char} K = p \neq 0$ ، زیرا حالت $\operatorname{char} K = 0$ بدیهی است.

(یک) به‌ازای هر $i > 1$ ، یک K ــ یکریختی مانند $\sigma : K(u_1) = K(u_i)$ با خاصیت $\sigma(u_1) = u_i$ وجود دارد که به K ــ یکریختی σ از F توسیع می‌شود (نتیجهٔ ۹۰۱ ، قضیهٔ ۸۰۳ ، و تمرین ۲۰۳) . چون $f \in K[x]$ ، بنابر قضیهٔ ۲۰۲ داریم

$$(x - u_1)^{r_1}\cdots(x - u_n)^{r_n} = f = \sigma f = (x - \sigma(u_1))^{r_1}\cdots(x - \sigma(u_n))^{r_n}.$$

چون $u_1, \ldots, u_n$ متمایز بوده و σ انژکتیو است، یکتایی تجزیه در $K[x]$ ایجاب می‌کند که $(x - u_i)^{r_i} = (x - \sigma(u_1))^{r_1}$ ، که از آنجا $r_1 = r_i$. این نشان می‌دهد که هر ریشهٔ f دارای بستایی $r = r_1$ است؛ درنتیجه ، $f = (x - u_1)^r\cdots(x - u_n)^r$ و $[K(u_1) : K] = \deg f = nr$. اما نتیجهٔ ۹۰۱ و قضیهٔ ۲۰۲ ایجاب می‌کنند که K ، n ــ تکریختی متمایز $K(u_1) \to F$ وجود داشته باشند ، که از آنجا ، طبق حکم ۱۲۰۶ و قضیهٔ ۱۴۰۳ ، $[K(u_1) : K]_s = n$. بنابراین ،

$$[K(u_1) : K]_i = [K(u_1) : K]/[K(u_1) : K]_s = nr/n = r.$$

(دو) چون r توانی از $p = \operatorname{char} K$ است ، داریم

$$f = (x - u_1)^r\cdots(x - u_n)^r = (x^r - u_1^r)\cdots(x^r - u_n^r).$$

لذا ، f یک چندجمله‌ای از x^r با ضرایب در $\bar{K}$ است؛ مثلاً " $f = \sum_{i=0}^{n} a_i x^{ri}$ " . درنتیجه ، u_1^r ریشه‌ای از $g(x) = \sum_{i=0}^{n} a_i x^i = (x - u_1^r)\cdots(x - u_n^r) \in K[x]$ می‌باشد . چون $u_1, \ldots, u_n$ متمایزند ، $g(x) \in K[x]$ جدایی‌پذیر است . بنابراین ، $u_1^r = u_1^{[K(u_1):K]_i}$ روی K جدایی‌پذیر می‌باشد .

نتیجهٔ زیر از مطلب فوق مستقل بوده و در آینده به کار نمی‌آید .

حکم ۱۵۰۶ (قضیهٔ عنصر اولیه). *فرض کنیم F یک توسیع میدان با بعد متناهی K باشد .*

(یک) هرگاه F روی K جدایی‌پذیر باشد، آنگاه F یک توسیع سادهٔ K است.
(دو) (آرتین) به‌طور کلی، F یک توسیع سادهٔ K است اگر و فقط اگر تنها تعدادی متناهی میدان میانی وجود داشته باشد.

تبصره. عنصر u با خاصیت $F = K(u)$ را **اولیه** می‌نامیم.

طرح برهان ۱۵.۶. بند اول برهان لم ۱۷.۳، که حتی اگر میدان K متناهی باشد نیز برقرار است، نشان می‌دهد که یک توسیع جدایی‌پذیر فقط تعدادی متناهی میدان میانی دارد. لذا، کافی است قسمت (دو) ثابت شود. چون (دو) بوضوح برای K متناهی برقرار است (نتیجهٔ ۸.۵)، فرض می‌کنیم K نامتناهی باشد. یک طرف (دو) در بند دوم برهان لم ۱۷.۳ ثابت شد. به عکس، فرض کنیم $F = K(u)$، که در آن u روی K جبری است (زیرا $[F : K]$ متناهی است). فرض کنیم E یک میدان میانی بوده و $g \in E[x]$ چندجمله‌ای تکین تحویل‌ناپذیر از u روی E باشد. هرگاه $g = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$، آنگاه $n = [F : E]$. با تحقیق اینکه $n = [F : K(a_0, \ldots, a_{n-1})]$، نشان دهید که $E = K(a_0, a_1, \ldots, a_{n-1})$. لذا، هر میدان میانی E به‌طور منحصر به فرد به وسیلهٔ چندجمله‌ای تکین تحویل‌ناپذیر g از u روی E معین می‌شود. هرگاه f چندجمله‌ای تحویل ناپذیر تکین از u روی K باشد، آنگاه، بنابر قضیهٔ ۶.۱، $g \mid f$. چون f در هر میدان تجزیه‌گر به طور منحصر به فرد تجزیه می‌شود (نتیجهٔ III ۴.۶۰)، f فقط می‌تواند تعدادی متناهی مقسوم علیه تکین متمایز داشته باشد. درنتیجه، فقط تعدادی متناهی میدان میانی وجود دارند.

تمرینات

تذکر. F همواره یک توسیع میدان از میدان K است مگر خلافش گفته شود.

۱. فرض کنید $\operatorname{char} K = p \neq 0$ و $n \geq 1$ چنان عدد صحیحی باشد که $(p,n) = 1$. هرگاه $v \in F$ و $nv \in K$، آنگاه $v \in K$.

۲. هرگاه $u \in F$ روی K صرفا" جدایی‌ناپذیر باشد، آنگاه u روی هر میدان میانی E صرفا" جدایی‌ناپذیر است. از اینرو، هرگاه F روی K صرفا" جدایی‌ناپذیر باشد، آنگاه F روی E صرفا" جدایی‌ناپذیر است.

۳ . هرگاه F روی‌میدان‌میانی E و E روی K صرفا "جدایی‌ناپذیر باشد ، آنگاه F روی K صرفا "جدایی‌ناپذیر است .

۴ . هرگاه $u \in F$ ، روی K جدایی‌پذیرو $v \in F$ روی K صرفا "جدایی‌ناپذیر باشد ، آنگاه $K(u,v) = K(u+v)$. هرگاه $u \neq 0, v \neq 0$ ، آنگاه $K(u,v) = K(uv)$.

۵ . هرگاه $\operatorname{char} K = p \neq 0$ و $a \in K$ ولی $a \notin K$ ، آنگاه $x^{p^n} - a \in K[x]$ به‌ازای هر $n > 1$ تحویل‌ناپذیر است .

۶ . هرگاه $f \in K[x]$ تکین تحویل‌ناپذیر بوده ، $\deg f \geq 2$ ، و همهٔ ریشه‌های f (در یک میدان تجزیه‌گر) مساوی باشند ، آنگاه $\operatorname{char} K = p \neq 0$ و ، به‌ازای $n \geq 1$ ی و $a \in K$ ای ، $f = x^{p^n} - a$.

۷ . فرض کنید F, K, S, P همانند در قضیهٔ ۷.۶ بوده و E یک میدان میانی باشد . در این صورت ،

(آ) F روی E صرفا "جدایی‌ناپذیر است اگر و فقط اگر $S \subset E$ ؛

(ب) هرگاه F روی E جدایی‌پذیر باشد ، آنگاه $P \subset E$ ؛

(پ) هرگاه $E \cap S = K$ ، آنگاه $E \subset P$ ،

۸ . هرگاه $\operatorname{char} K = p \neq 0$ و $[F : K]$ متناهی بوده ولی بر p بخشپذیر نباشد ، آنگاه F روی K جدایی‌پذیر است .

۹ . فرض کنید $\operatorname{char} K = p \neq 0$. دراین‌صورت ، عنصرجبری $u \in F$ روی K جدایی‌پذیر است اگر و فقط اگر به‌ازای هر $n \geq 1$ ، $K(u) = K(u^{p^n})$.

۱۰ . فرض کنید $\operatorname{char} K = p \neq 0$ و $f \in K[x]$ تحویل‌ناپذیر از درجهٔ n باشد . همچنین ، m بزرگترین عدد صحیح نامنفی باشد که f یک چندجمله‌ای از x^{p^m} است ولی یک چندجمله‌ای از $x^{p^{m+1}}$ نیست . دراین صورت ، $n = n_0 p^m$. هرگاه u ریشه‌ای از f باشد ، آنگاه $[K(u) : K]_s = n_0$ و $[K(u) : K]_i = p^m$.

۱۱ . هرگاه $f \in K[x]$ تحویل‌ناپذیر و از درجهٔ $m > 0$ بوده و $\operatorname{char} K$ ، m را عاد نکند ، آنگاه f جدایی‌پذیر است .

۱۲ . F روی K صرفا "جدایی‌ناپذیراست اگر و فقط اگر F روی K جبری بوده و ، به‌ازای هر توسیع میدان E از F ، تنها K ــ تکریختی $F \to E$ نگاشت شمول باشد .

۱۳ . (آ) شرایط زیر بر میدان K باهم معادلند :

(یک) هر چندجمله‌ای تحویل‌ناپذیر در $K[x]$ جدایی‌پذیر است ؛

(دو) هر بست جبری $\bar{K}$ از K روی K گالواست؛
(سه) هر توسیع میدان جبری K روی K جدایی‌پذیر است؛
(چهار) یا $\operatorname{char} K = 0$ یا $\operatorname{char} K = p$ و $K = K^p$.
میدان K ی صادق در (یک) تا (چهار) *کامل* نام دارد.
(ب) هر میدان متناهی کامل است.

۱۴ . هرگاه $F = K(u,v)$ ، که در آن u,v روی K جبری بوده و u روی K جدایی‌پذیر است، آنگاه F یک توسیع سادهٔ K می‌باشد.

۱۵ . فرض کنید $\operatorname{char} K = p \neq 0$ و نیز $F = K(u,v)$ ، که در آن $u^p \in K$ ، $v^p \in K$ ، و $[F:K] = p^2$. در این صورت، F یک توسیع سادهٔ K نیست. تعدادی نامتناهی میدان میانی ارائه دهید.

۱۶ . فرض کنید F یک توسیع جبری K باشد به‌طوری‌که هر چندجمله‌ای در $K[x]$ ریشه‌ای در F دارد. در این صورت، F بست جبری K است. [**راهنمایی.** قضایای ۱۴۰۳ و ۷۰۶ و حکم ۱۵۰۶ ممکن است مفید باشند.]

۷ توسیعهای دوری

ایدهٔ اصلی در بخشهای ۷ تا ۹ تحلیل توسیعهای میدان گالوایی است که گروههای گالوای آنها ساختار مقرری دارند (مثلاً "، دوری یا حلپذیرند). در این بخش اغلب توسیعهای گالوای با بعد متناهی و دارای گروههای گالوای دوری را توصیف می‌کنیم (احکام ۷۰۷ و ۸۰۷؛ قضیهٔ ۱۱۰۷). برای این کار، ابتدا باید چند مطلب در باب اثر و نرم را یاد بگیریم.

تعریف ۱۰۷ . فرض کنیم F یک توسیع میدان با بعد متناهی از K بوده و $\bar{K}$ یک بست جبری K شامل F باشد. همچنین، $\sigma_1, \ldots, \sigma_r$ تمام K ــ تکریختیهای متمایز $F \to \bar{K}$ باشند. اگر $u \in F$ ، نرم u ، که با $N_K^F(u)$ نموده می‌شود، عنصر

$$N_K^F(u) = (\sigma_1(u)\sigma_2(u)\cdots\sigma_r(u))^{[F:K]_i}$$

می‌باشد. *اثر* u ، که با $T_K^F(u)$ نموده می‌شود، عنصر

$$T_K^F(u) = [F:K]_i(\sigma_1(u) + \sigma_2(u) + \cdots + \sigma_r(u))$$

خواهد بود.

چند تبصره. قضیهٔ ۲۰۷ زیر نشان می‌دهد که تعریف به انتخاب $\bar{K}$ بستگی ندارد. می‌توان نشان داد که اگر $\bar{K}$ با توسیع نرمالی از K شامل F عوض شود، تعریف معادل دیگری به دست می‌آید (تمرین ۱). $\bar{K}$ روی K نرمال است (قضایای ۴۰۳ و ۱۴۰۳)، که از آنجا، طبق حکم ۱۲۰۶، $r = [F:K]_s$ متناهی می‌باشد. اگر از قراین معلوم باشد، گاهی N_K^F و T_K^F را فقط به صورت N و T می‌نویسیم.

توجه کنید که اثر اساساً "مشابه جمعی نرم است. این بدان معنی است که در بسیاری از حالات برهانی مستلزم یکی مستقیماً "به برهانی از مطلب مشابه برای دیگری تبدیل می‌شود. اما استثناهایی نیز وجود دارند. مثلاً "، هرگاه F روی K جدایی‌پذیر نباشد، آنگاه $\operatorname{char} K = p \neq 0$ و $[F:K]_s = p^t$ $(t \geq 1)$. درنتیجه، به‌ازای هر $u \in F$، $T_K^F(u) = 0$، ولی $N_K^F(u)$ ممکن است صفر نباشد.

مثال. فرض کنیم $F = \mathbf{C}$ و $K = \mathbf{R}$ و $\bar{K} = \mathbf{C}$ را اختیار کرده باشیم. به‌آسانی معلوم می‌شود که تنها $\mathbf{R}$ ـ تکریختیهای $\mathbf{C} \to \mathbf{C}$ همانی و تزویج مختلط است. درنتیجه،

$$N(a + bi) = [(a + bi)(a - bi)]^1 = a^2 + b^2.$$

کاربردهای اصلی نرم و اثر که در اینجا داده می‌شود وقتی است که F روی K گالوا باشد. در این حالت گروه گالوا متناهی است و توصیف مناسبتری از نرم و اثر وجود دارد، که گاهی به عنوان تعریف گرفته می‌شود.

قضیهٔ ۲۰۷. *هرگاه* F *یک توسیع میدان گالوا با بعد متناهی از* K *بوده و*

$$Aut_K F = \{\sigma_1, \ldots, \sigma_n\},$$

آنگاه، به‌ازای هر $u \in F$،

$$N_K^F(u) = \sigma_1(u)\sigma_2(u)\cdots\sigma_n(u);$$

و

$$T_K^F(u) = \sigma_1(u) + \sigma_2(u) + \cdots + \sigma_n(u).$$

برهان. فرض کنیم $\bar{K}$ یک بسط جبری K شامل F باشد. چون F روی K نرمال است

(نتیجهٔ ۱۵۰۳) ، بنابرقضیهٔ ۱۴۰۳ ، K ــ تکریختیهای $F \to \bar{K}$ درست‌عناصر $\mathrm{Aut}_K F$ اند . چون F نیز روی K جدایی‌پذیراست (نتیجهٔ ۱۵۰۳) ، $[F:K]_i = 1$. حال‌قضیه مستقیما" از تعریف ۱۰۷ نتیجه خواهد شد .

فرض‌کنیم F روی K گالوابوده‌و $\mathrm{Aut}_K F = \{\sigma_1, \ldots, \sigma_n\}$. چون $\mathrm{Aut}_K F$ گروه‌است ، عناصر $\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n$ (به‌ازای‌هر $\sigma_i \in \mathrm{Aut}_K F$ ثابت) چیزی‌جز $\sigma_1, \sigma_2, \ldots, \sigma_n$ احتمالا" با ترتیبی متفاوت نیستند . این ایجاب می‌کند که به‌ازای هر $u \in F$ ، $N_K^F(u)$ و $T_K^F(u)$ به وسیلهٔ هر $\sigma_i \in \mathrm{Aut}_K F$ ثابت بمانند . بنابراین ، $N_K^F(u)$ و $T_K^F(u)$ باید در K باشند . قضیهٔ زیر نشان می‌دهد که این حتی اگر F روی K گالوا نباشد درست است . دو قسمت اول بارها مورد استفاده قرار می‌گیرند ؛ **دوقسمت آخر در آینده به کار نخواهند آمد.**

قضیهٔ ۳۰۷ . *فرض‌کنیم F یک‌توسیع‌میدان با بعد متناهی از K باشد . در این صورت ، به‌ازای هر $u,v \in F$ ،*

(یک) $T_K^F(u) + T_K^F(v) = T_K^F(u+v)$ و $N_K^F(u)N_K^F(v) = N_K^F(uv)$ ؛

(دو) هرگاه $u \in K$ ، *آنگاه* $N_K^F(u) = u^{[F:K]}$ و $T_K^F(u) = [F:K]u$ ؛

(سه) $N_K^F(u)$ و $T_K^F(u)$ *عناصری از* K *اند . به‌طور دقیقتر ،*

$$N_K^F(u) = ((-1)^n a_0)^{[F:K(u)]} \in K \quad \text{و} \quad T_K^F(u) = -[F:K(u)]a_{n-1} \in K$$

که در آن $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ *چندجمله‌ای تحویل‌ناپذیر از* u *است* ؛

(چهار) هرگاه E *یک میدان میانی باشد ، آنگاه*

$$N_K^E(N_E^F(u)) = N_K^F(u) \quad \text{و} \quad T_K^E(T_E^F(u)) = T_K^F(u) .$$

طرح برهان . (یک) و (دو) مستقیما" از تعریف ۱۰۷ و این امر که $r = [F:K]_s$ و $[F:K] = [F:K]_s[F:K]_i$ نتیجه می‌شود .

(سه) فرض‌کنیم $E = K(u)$. بست جبری $\bar{K}$ از K که شامل F باشد یک بست جبری E نیز هست . برهان لم ۱۱۰۶ نشان می‌دهد که K ــ تکریختیهای متمایز $F \to \bar{K}$ دقیقا" نگاشتهای $\sigma_k\tau_j$ $(1 \le k \le t; 1 \le j \le r)$ می‌باشند ، که در آنها σ ها همهٔ K ــ خودریختیهایی از $\bar{K}$ هستند که تحدید آنها به E متمایز بوده‌و τ ها همهٔ E ــ تکریختیهای متمایز $F \to \bar{K}$ می‌باشند . لذا ، طبق حکم ۱۲۰۶ ، $t = [E:K]_s$ ، که

از آنجا $n = [E:K] = t[E:K]_i$ (نتیجهٔ ۱۳۰۶).

با استفاده از (دو) و نتیجهٔ ۱۳۰۶، نشان‌دهیدکه

$$N_K{}^F(u) = \left(\prod_{k=1}^{t} \sigma_k(u)\right)^{[F:E][E:K]_i} \quad \text{و} \quad T_K{}^F(u) = [F:E][E:K]_i\left(\sum_{k=1}^{t} \sigma_k(u)\right).$$

چون $\sigma_i : K(u) \cong K(\sigma_i(u))$، نتیجهٔ ۹۰۱ ایجاب خواهد کرد که $\sigma_1(u), \ldots, \sigma_t(u)$ همهٔ ریشه‌های متمایز f می‌باشند. بنابر نتیجهٔ ۱۴۰۶،

$$f = [(x-\sigma_1(u))(x-\sigma_2(u))\cdots(x-\sigma_t(u))]^{[E:K]_i}$$
$$= \left[x^t - \left(\sum_{k=1}^{t}\sigma_k(u)\right)x^{t-1} + \cdots + \left((-1)^t \prod_{k=1}^{t}\sigma_k(u)\right)\right]^{[E:K]_i}.$$

هرگاه $[E:K]_i = 1$، آنگاه $n = t$ و نتیجه فورا "حاصل است. هرگاه $[E:K]_i > 1$، آنگاه $[E:K]_i$ توان مثبتی از $p = \text{char } K$ است. محاسبهٔ a_0 و نیز اثبات $a_{n-1} = 0 = T_K{}^F(u)$ آسان است؛ از تمرین III ۱۱۰۱۰ استفاده کنید.

(چهار) از نمادگذاری‌بنداول برهان (سه) استفاده کرده، E را میدان میانی *دلخواهی* بگیرید. تعاریف مناسبی به کار برده و از نتیجهٔ ۱۳۰۶ استفاده نمایید.

علاوه بر اثر و نرم، تعریف زیر نیز لازم خواهد شد.

تعریف ۴۰۷. فرض‌کنیم S مجموعه‌ای نـاتهی از خـودریختیهای میدان F باشد. S *مستقل خطی* است مشروط بر اینکه به‌ازای هر $a_1, \ldots, a_n \in F$ و $\sigma_1, \ldots, \sigma_n \in S$ $(n \geq 1)$، به‌ازای هر i، $a_i = 0 \Rightarrow$ به‌ازای هر $u \in F$، $a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0$.

لم ۵۰۷. *هرگاه S مجموعه‌ای از خودریختیهای متمایز میدان F باشد، آنگاه S مستقل خطی می‌باشد.*

برهان. هرگاه S مستقل خطی نباشد، آنگاه $a_i \in F$ هایی ناصفر و $\sigma_i \in S$ هایی متمایز وجود دارند به‌طوری‌که

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0 \quad \text{، به‌ازای هر } u \in F. \qquad (1)$$

از میان همهٔ این "روابط وابستگی" یکی را با n مینیمال اختیار می‌کنیم؛ واضح است که

$n > 1$. چون σ_1 و σ_2 متمایزند ، $v \in F$ ای‌وجوددارد‌که $\sigma_1(v) \neq \sigma_2(v)$. با اعمال (۱) بر عنصر uv (به‌ازای هر $u \in F$) ، نتیجه می‌شود که

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_2(v) + \cdots + a_n\sigma_n(u)\sigma_n(v) = 0; \qquad (۲)$$

و با ضرب (۱) در $\sigma_1(v)$ نتیجه می‌شود که

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_1(v) + \cdots + a_n\sigma_n(u)\sigma_1(v) = 0. \qquad (۳)$$

تفاضل (۲) و (۳) رابطهٔ زیر است: به‌ازای هر $u \in F$ ،

$$a_2[\sigma_2(v) - \sigma_1(v)]\sigma_2(u) + a_3[\sigma_3(v) - \sigma_1(v)]\sigma_3(u) + \cdots + a_n[\sigma_n(v) - \sigma_1(v)]\sigma_n(u) = 0.$$

چون $a_2 \neq 0$ و $\sigma_2(v) \neq \sigma_1(v)$ ، همهٔ ضرایب صفرنیستندو این مینیمالی n را نقض می‌کند.

توسیع میدان F از میدان K را **دوری** [آبلی] گویند اگر F روی K جبری و گالوا بوده و $\mathrm{Aut}_K F$ یک گروه دوری [آبلی] باشد . هرگاه در این وضع $\mathrm{Aut}_K F$ یک گروه دوری متناهی از مرتبهٔ n باشد ، آنگاه گوییم F یک **توسیع دوری از درجهٔ n** است (و ، بنابر قضیهٔ اساسی ۵۰۲ ، $[F : K] = n$) . مثلاً " ، قضیهٔ ۱۰۰۵ می‌گوید هر توسیع با بعد متناهی یک میدان متناهی یک توسیع دوری است . قضیهٔ زیر ارتباط مهم بین توسیعهای دوری و نرم و اثر را بازگو می‌کند .

قضیهٔ ۶۰۷ . *فرض کنیم F یک‌توسیع میدان دوری K از درجهٔ n بوده ، σ مولدی از $\mathrm{Aut}_K F$ باشد ، و $u \in F$. در این صورت ،*

(یک) $T_K^F(u) = 0$ *اگر و فقط اگر به‌ازای* $v \in F$ *ای ،* $u = v - \sigma(v)$ ؛

(دو) (قضیهٔ 90 هیلبرت) $N_K^F(u) = 1_K$ *اگر و فقط اگر به‌ازای* $v \in F$ *ای ناصفر ،* $u = v\sigma(v)^{-1}$.

طرح برهان . برای راحتی می‌نویسیم $\sigma(x) = \sigma x$. چون σ ، $\mathrm{Aut}_K F$ را تولید می‌کند ، مرتبه‌اش n است ، و $\sigma, \sigma^2, \sigma^3, \ldots, \sigma^{n-1}, \sigma^n = 1_F = \sigma^0$ ، n خودریختی متمایز F می‌باشند . بنابر قضیهٔ ۲۰۷ ، $T(u) = u + \sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u$ و $N(u) = u(\sigma u)(\sigma^2 u)\cdots(\sigma^{n-1}u)$.

(یک) هرگاه $u = v - \sigma v$ ، آنگاه با استفاده از تعریف و اینکه

$$\sigma^n(v) = v \quad \text{و} \quad T(v - \sigma v) = T(v) - T(\sigma v)$$

نشان دهید که $T(u) = 0$. به‌عکس، فرض کنیم $T(u) = 0$. به طریق زیر $w \in F$ را طوری

اختیار می‌کنیم که $T(w) = 1_K$. بنابرلم ۵۰۷ (چون $1_K \neq 0$) ، $z \in F$ ی هست به‌طوری‌که

$$0 \neq 1_K z + \sigma z + \sigma^2 z + \cdots + \sigma^{n-1} z = T(z).$$

چون بنابر تبصره‌های بعد از قضیهٔ ۲۰۷ $T(z) \in K$ ، داریم

$$\sigma[T(z)^{-1}z] = T(z)^{-1}\sigma(z)$$

درنتیجه ، هرگاه $w = T(z)^{-1}z$ ، آنگاه

$$\begin{aligned} T(w) &= T(z)^{-1}z + T(z)^{-1}\sigma z + \cdots + T(z)^{-1}\sigma^{n-1}z \\ &= T(z)^{-1}T(z) = 1_K. \end{aligned}$$

حال فرض کنیم

$$\begin{aligned} v = {} & uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) \\ & + (u + \sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 w) + \cdots + (u + \sigma u + \cdots + \sigma^{n-2}u)(\sigma^{n-2}w). \end{aligned}$$

با استفاده از خودریختی بودن σ و اینکه

$$0 = T(u) = u + \sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u$$

که رابطهٔ $u = -(\sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u)$ را ایجاب می‌کند ، نشان دهید که

$$\begin{aligned} v - \sigma v = {} & uw + u(\sigma w) + u(\sigma^2 w) + u(\sigma^3 w) + \cdots + u(\sigma^{n-2}w) \\ & + u(\sigma^{n-1}w) = uT(w) = u1_K = u. \end{aligned}$$

(دو) هرگاه $u = v\sigma(v)^{-1}$ ، آنگاه چون σ یک‌خودریختی از مرتبهٔ n است ، $\sigma^n(v^{-1}) = v^{-1}$ ، $\sigma(v^{-1}) = \sigma(v)^{-1}$ و ، به‌ازای هر $1 \leq i \leq n-1$ ، $\sigma^i(v)\sigma^{i+1}(v)^{-1}$. از اینرو ،

$$N(u) = (v\sigma(v)^{-1})(\sigma v\sigma^2(v)^{-1})(\sigma^2 v\sigma^3(v)^{-1})\cdots(\sigma^{n-1}v\sigma^n(v)^{-1}) = 1_K$$

به عکس، فرض کنیم $N(u) = 1_K$ ،کهایجاب می‌کند که $u \neq 0$. بنابر لم ۵۰۷ ، $y \in F$ ی هست به‌طوری که عنصر v داده شده با

$$\begin{aligned} v = {} & uy + (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + \cdots + (u\sigma u\cdots\sigma^{n-2}u)\sigma^{n-2}y \\ & + (u\sigma u\cdots\sigma^{n-1}u)\sigma^{n-1}y \end{aligned}$$

ناصفراست.چون‌آخرین جمعوند v مساوی $N(u)\sigma^{n-1}y = 1_K\sigma^{n-1}y = \sigma^{n-1}y$ است ، به آسانی تحقیق می‌شود که $u^{-1}v = \sigma v$ ، که از آنجا $\sigma(v) \neq 0$ $(u = v\sigma(v)^{-1}$ ، زیرا $v \neq 0$ و σ انژکتیو است .

حال تمام ابزار لازم برای تحلیل توسیعهای دوری در دست است . مطلب را با تحویل مسئله به شکل ساده‌تر آغاز می‌کنیم .

حکم ۷.۷ . فرض کنیم F یک توسیع میدان دوری K از درجهٔ n بوده و $n = mp^t$ ، که در آن $p = char\ K \neq 0$ و $(m,p) = 1$. در این صورت ، زنجیری از میدانهای میانی مانند $F \supset E_0 \supset E_1 \supset \cdots \supset E_{t-1} \supset E_t = K$ وجود دارد به‌طوری‌که F یک توسیع دوری E_0 از درجهٔ m بوده و ، به‌ازای هر مقدار $0 \leq i \leq t$ ، E_{i-1} یک توسیع دوری E_i از درجهٔ p است .

طرح برهان . طبق فرض، F روی K گالوابوده و $\mathrm{Aut}_K F$ دوری (آبلی) است ؛ درنتیجه ، هر زیرگروه نرمال است . به یاد آورید که هر زیرگروه و گروه خارج‌قسمتی یک گروه دوری دوری است (قضیهٔ I ۵.۳۰) . درنتیجه ، قضیهٔ اساسی ۵.۲ (دو) ایجاب می‌کند که به‌ازای هر میدان میانی E ، F روی E و E روی K دوری است . پس نتیجه می‌شود که به‌ازای هر جفت L,M از میدانهای میانی که $L \subset M$ ، M یک توسیع دوری L می‌باشد ؛ بخصوص، M روی L گالوای جبری می‌باشد .

فرض کنیم H زیرگروه (دوری) منحصر به‌فردی از مرتبهٔ m از $\mathrm{Aut}_K F$ بوده (تمرین I ۶.۳۰) و E_0 میدان ثابت آن باشد (درنتیجه ، $H = H'' = E_0' = \mathrm{Aut}_{E_0} F$) . در این صورت ، F روی E_0 دوری از درجهٔ m و E_0 روی K دوری از درجهٔ p^t است . چون $\mathrm{Aut}_K E_0$ دوری از مرتبهٔ p^t است ، زنجیری از زیرگروهها مانند

$$1 = G_0 < G_1 < G_2 < \cdots < G_{t-1} < G_t = \mathrm{Aut}_K E_0$$

دارد ، که $|G_i| = p^i$ ، $[G_i : G_{i-1}] = p$ ، و G_i/G_{i-1} دوری‌ازمرتبهٔ p است (ر.ک. قضیهٔ I ۴.۳۰ (هفت)) . به‌ازای هر i ، E_i را میدان ثابت G_i (نسبت به E_0 و $\mathrm{Aut}_K E_0$) می‌گیریم . قضیهٔ اساسی ۵.۲ ایجاب می‌کند که

(یک) $E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_{t-1} \supset E_t = K$ ؛ (دو) $[E_{i-1} : E_i] = [G_i : G_{i-1}] = p$ ؛ و (سه) $\mathrm{Aut}_{E_i} E_{i-1} \cong G_i/G_{i-1}$.

بنابراین ، E_{i-1} یک توسیع دوری E_i از درجهٔ p است $(0 \leq i \leq t-1)$.

فرض کنیم F یک توسیع میدان دوری K از درجهٔ n باشد . در پرتو حکم ۷.۷ می‌توان ، دست‌کم در اصول ، فقط به‌دوحالت‌زیرپرداخت : (یک) $n = \mathrm{char}\ K = p \neq 0$ ؛ (دو) $\mathrm{char}\ K = 0$ یا $\mathrm{char}\ K = p \neq 0$ و $(p,n) = 1$ (یعنی ، $\mathrm{char}\ K \nmid n$) .اولین حالت در حکم زیر مطرح می‌شود .

حکم ۸۰۷ . *فرض کنیم K یک میدان با مشخص $p \neq 0$ باشد . F یک توسیع میدان دوری از K با درجهٔ p است اگر و فقط اگر F یک میدان تجزیه‌گر یک چندجمله‌ای تحویل‌ناپذیر به شکل $x^p - x - a \in K[x]$ روی K باشد . در این حالت $F = K(u)$ ، که در آن u ریشه‌ای از $x^p - x - a$ است .*

برهان . ($\Rightarrow$) هرگاه σ مولدی از گروه دوری $\mathrm{Aut}_K F$ باشد ، آنگاه ، طبق قضیهٔ ۳۰۷ (دو) ،

$$T_K^F(1_K) = [F : K]1_K = p1_K = 0$$

که از آنجا ، بنابر قضیهٔ ۶۰۷ (یک) ، به‌ازای $v \in F$ ای ، $1_K = v - \sigma(v)$. هرگاه $u = -v$ ، آنگاه $\sigma(u) = u + 1_K \neq u$ ، که از آنجا $u \notin K$. چون $[F : K] = p$ ، میدان میانی وجود ندارد ، و باید داشته باشیم $F = K(u)$. توجه کنید که

$$\sigma(u^p) = (u + 1_K)^p = u^p + 1_K^p = u^p + 1_K$$

که ایجاب می‌کند که $\sigma(u^p - u) = (u^p + 1_K) - (u + 1_K) = u^p - u$. چون F روی K گالوا بوده و $\mathrm{Aut}_K F = \langle \sigma \rangle$ ، باید $a = u^p - u$ در K باشد . بنابراین ، u ریشه‌ای از $x^p - x - a \in K[x]$ است ، که لزوما "چندجمله‌ای تحویل‌ناپذیر برای u روی K است ، زیرا درجهٔ u روی K مساوی $[K(u) : K] = [F : K] = p$ می‌باشد .

به یاد آورید که زیرمیدان اول Z_p از K از p عنصر متمایز

$$0, 1 = 1_K, 2 = 1_K + 1_K, \ldots, p - 1 = 1_K + \cdots + 1_K$$

تشکیل شده است (قضیهٔ ۱۰۵) . بند اول برهان قضیهٔ ۶۰۵ نشان می‌دهد که به‌ازای هر $i \in Z_p$ ، $i^p = i$. چون u ریشه‌ای از $x^p - x - a$ است ، به‌ازای هر $i \in Z_p$ داریم

$$(u + i)^p - (u + i) - a = u^p + i^p - u - i - a = (u^p - u - a) + (i^p - i) = 0 + 0 = 0$$

لذا ، $u + i \in K(u) = F$ ، به‌ازای هر $i \in Z_p$ ، ریشه‌ای از $x^p - x - a$ است ، که از آنجا F شامل p ریشهٔ متمایز $x^p - x - a$ است . بنابراین ، $F = K(u)$ یک میدان تجزیه‌گر روی K ی $x^p - x - a$ است . بالاخره ، هرگاه $u + i$ $(i \in Z_p \subset K)$ ریشه‌ای از $x^p - x - a$ باشد ، آنگاه بوضوح $K(u + i) = K(u) = F$.

($\Leftarrow$) فرض کنیم F یک میدان تجزیه‌گر $x^p - x' - a \in K[x]$ روی K باشد . فرض نمی‌کنیم $x^p - x - a$ تحویل‌ناپذیر است و چیزی بیش از آنچه قضیه گفته ثابت می‌کنیم . هرگاه u ریشه‌ای از $x^p - x - a$ باشد ، آنگاه بند پیش نشان می‌دهد که $K(u)$ شامل p ریشهٔ متمایز $x^p - x - a$ است . $u, u + 1, \ldots, u + (p - 1) \in K(u)$. اما $x^p - x - a$ حداکثر

p ریشه در F دارد و این ریشه‌ها F را روی K تولید می‌کنند. بنابراین، $F = K(u)$، عوامل تحویل‌ناپذیر $x^p - x - a$ جدایی‌پذیرند، و F روی K گالوا می‌باشد (قضیهٔ ۱۱۰۳ و تمرین ۱۳۰۳). هر $\tau \in \mathrm{Aut}_K F = \mathrm{Aut}_K K(u)$ کاملا "به‌وسیلهٔ $\tau(u)$ معین می‌شود. قضیهٔ ۲۰۲ ایجاب می‌کند که به‌ازای $i \in Z_p \subset K$ ی، $\tau(u) = u + i$. تحقیق کنید که انتساب $\tau \mapsto i$ یک تکریختی گروهها مانند $\theta : \mathrm{Aut}_K F \to Z_p$ را تعریف می‌کند. درنتیجه، $\mathrm{Aut}_K F \cong \mathrm{Im}\,\theta$ یا 1 است یا Z_p. هرگاه $\mathrm{Aut}_K F = 1$، آنگاه، بنابر قضیهٔ اساسی ۵۰۲، $[F : K] = 1$، که ازآنجا $u \in K$ و $x^p - x - a$ در $K[x]$ تجزیه می‌شود. لذا، اگر $x^p - x - a$ روی K تحویل‌ناپذیر باشد، باید داشته باشیم $\mathrm{Aut}_K F \cong Z_p$. لذا، در این حالت، F روی K دوری از درجهٔ p است.

نتیجهٔ ۹۰۷. هرگاه K یک میدان با مشخص $p \neq 0$ بوده و $x^p - x - a \in K[x]$، آنگاه $x^p - x - a$ یا تحویل‌ناپذیر است یا در $K[x]$ تجزیه می‌شود.

برهان. از نمادگذاری حکم ۸۰۷ استفاده می‌کنیم. در پرتو آخرین بند برهان، کافی است ثابت کنیم هرگاه $\mathrm{Aut}_K F \cong \mathrm{Im}\,\theta = Z_p$، آنگاه $x^p - x - a$ تحویل‌ناپذیر است. هرگاه u و i $(i \in Z_p \subset K)$ ریشه‌های $x^p - x - a$ باشند، آنگاه $\tau \in \mathrm{Aut}_K F$ ای وجود دارد به‌طوری‌که $\tau(u) = v$؛ و درنتیجه، $\tau : K(u) \cong K(v)$ (τ را با خاصیت $\theta(\tau) = i$ اختیارمی‌کنیم). بنابراین، u و v ریشه‌های یک چندجمله‌ای تحویل‌ناپذیر در $K[x]$ اند (نتیجهٔ ۹۰۱). چون v دلخواه بود، این ایجاب می‌کند که $x^p - x - a$ تحویل‌ناپذیر باشد.

حکم ۸۰۷ ساختار یک توسیع دوری از نوع اول‌مذکوردر ص ۴۶۰ را کاملا "توصیف می‌کند. برای تعیین ساختار یک توسیع دوری از درجهٔ n از نوع دوم، باید بر میدان زمینهٔ K فرضی اضافی گذاشت.

فرض کنیم K یک میدان بوده و n عدد صحیح مثبتی باشد. گوییم عنصر $\xi \in K$ یک **ریشهٔ n م واحد** است مشروط بر اینکه $\xi^n = 1_K$ (یعنی، ξ یک ریشهٔ $x^n - 1_K \in K[x]$ باشد). به آسانی معلوم می‌شود که مجموعهٔ تمام ریشه‌های n م واحد در K یک زیرگروه ضربی گروه ضربی عناصر ناصفر K را تشکیل می‌دهند. بنابر قضیهٔ ۳۰۵، این زیرگروه

دوری است و، طبق قضیهٔ III ۷.۶۰، مرتبه‌اش حداکثر n است. گوییم $\zeta \in K$ یک **ریشهٔ n م اولیهٔ واحد** است مشروط بر اینکه ζ یک ریشهٔ n م واحد بوده و ζ در گروه ضربی ریشه‌های n م واحد از مرتبهٔ n باشد. بخصوص، یک ریشهٔ n م اولیهٔ واحد گروه دوری تمام ریشه‌های n م واحد را تولید می‌کند.

چند تبصره. هرگاه $\operatorname{char} K = p$ و $p \mid n$، آنگاه $n = p^k m$، که در آن $(p,m) = 1$ و $m < n$. لذا، $x^n - 1_K = (x^m - 1_K)^{p^k}$ (تمرین III ۱۱.۱۰). درنتیجه، ریشه‌های n م واحد در K با ریشه‌های m م واحد در K یکی هستند. چون $m < n$، هیچ ریشهٔ n م اولیهٔ واحد در K وجود ندارد. به عکس، هرگاه $\operatorname{char} K \nmid n$ (بخصوص، هرگاه $\operatorname{char} K = 0$)، آنگاه $nx^{n-1} \neq 0$، که از آنجا $x^n - 1_K$ نسبت به مشتقش اول است. بنابراین، $x^n - 1_K$ دارای n ریشهٔ متمایز درمیدان تجزیه‌گر F از $x^n - 1_K$ روی K است (قضیهٔ III ۱۰.۶۰). لذا، گروه دوری ریشه‌های n م واحد در F دارای مرتبهٔ n بوده و F (ولی نه لزوماً K) شامل یک ریشهٔ n م اولیهٔ واحد است. توجه کنید هرگاه K شامل یک ریشهٔ n م اولیهٔ واحد باشد، آنگاه K شامل n ریشهٔ متمایز از $x^n - 1_K$ می‌باشد، که از آنجا $F = K$.

چند مثال. به‌ازای هر $n \geq 1$، 1_K یک ریشهٔ n م واحد در میدان K است. هرگاه $\operatorname{char} K = p \neq 0$ و $n = p^k$، آنگاه 1_K تنها ریشهٔ n م واحد در K است. زیر میدان $\mathbf{Q}(i)$ از $\mathbf{C}$ شامل هر دو ریشهٔ چهارم اولیهٔ واحد $(\pm i)$ است ولی شامل هیچ ریشهٔ سوم واحد جز 1 نیست (سایرین عبارتند از $-1/2 \pm \sqrt{3}\, i/2$). به‌ازای هر $n > 0$، $e^{2\pi i/n} \in \mathbf{C}$ یک ریشهٔ n م اولیهٔ واحد است.

برای اتمام توصیف خود از توسیعهای دوری، به لم زیر نیاز داریم.

لم ۱۰.۷. *فرض کنیم n یک عدد صحیح مثبت بوده و K میدانی باشد که شامل یک ریشهٔ n م اولیهٔ واحد ζ است.*

(یک) هرگاه $d \mid n$، آنگاه $\eta = \zeta^{n/d}$ یک ریشهٔ d ام اولیهٔ واحد در K است.

(دو) هرگاه $d \mid n$ و u یک ریشهٔ ناصفر $x^d - a \in K[x]$ باشد، آنگاه $x^d - a$ دارای d ریشهٔ

متمایز است؛ یعنی، $u, \eta u, \eta^2 u, \ldots, \eta^{d-1}u$، که در آنها $\eta \in K$ یک ریشهٔ d ام اولیهٔ واحد است. به علاوه، $K(u)$ یک میدان تجزیه‌گر $x^d - a$ روی K بوده و روی K گالوا می‌باشد.

برهان. (یک) طبق تعریف، ζ یک گروه دوری ضربی از مرتبهٔ n تولید می‌کند. هرگاه $d \mid n$، آنگاه، طبق قضیهٔ I ۴.۳.۰، $\eta = \zeta^{n/d}$ دارای مرتبهٔ d است، که از آنجا η یک ریشهٔ d ام اولیهٔ واحد می‌باشد.

(دو) هرگاه u ریشه‌ای از $x^d - a$ باشد، آنگاه $\eta^i u$ نیز چنین است. عناصر $\eta^0 = 1_K, \eta, \ldots, \eta^{d-1}$ متمایزند (قضیهٔ I ۴.۳.۰). درنتیجه، چون $\eta \in K$، ریشه‌های $u, \eta u, \ldots, \eta^{d-1}u$ از $x^d - a$ عناصر متمایزی از $K(u)$ اند. لذا، $K(u)$ یک میدان تجزیه‌گر $x^d - a$ روی K است. عوامل تحویل‌ناپذیر $x^d - a$ جدایی‌پذیرند، زیرا تمام ریشه‌ها متمایزند، که از آنجا، طبق قضیهٔ ۱۱.۳ و تمرین ۱۳.۳، $K(u)$ روی K گالوا است.

قضیهٔ ۱۱.۷. *فرض کنیم n یک عدد صحیح مثبت بوده و K میدانی باشد که شامل یک ریشهٔ n م اولیهٔ واحد ζ است. در این صورت، شرایط زیر بر توسیع میدان F از K باهم معادلند:*

(یک) *F دوری از درجهٔ d است، که $d \mid n$؛*

(دو) *F یک میدان تجزیه‌گر یک چندجمله‌ای به شکل $x^n - a \in K[x]$ روی K است (که در این حالت، به‌ازای هر ریشهٔ u از $x^n - a$، $F = K(u)$)؛*

(سه) *F یک میدان تجزیه‌گر یک چندجمله‌ای تحویل‌ناپذیر به شکل $x^d - b \in K[x]$ روی K است، که در آن $d \mid n$ (که در این حالت، به‌ازای هر ریشهٔ v از $x^d - b$، $F = K(v)$).*

برهان. (یک) $\Rightarrow$ (دو) لم ۱۰.۷ نشان می‌دهد که، به‌ازای هر ریشهٔ u از $x^n - a$، $F = K(u)$ و F روی K گالواست. هرگاه $\sigma \in \mathrm{Aut}_K F = \mathrm{Aut}_K K(u)$، آنگاه σ کاملا" به وسیلهٔ $\sigma(u)$ معین می‌شود، که بنابر قضیهٔ ۲.۲ ریشه‌ای از $x^n - a$ است. بنابراین، طبق لم ۱۰.۷، به‌ازای i ی $(0 \le i \le n-1)$، $\sigma(u) = \zeta^i u$. تحقیق کنید که انتساب $\sigma \mapsto \zeta^i$ یک تکریختی از $\mathrm{Aut}_K F$ به گروه دوری ضربی (از مرتبهٔ n) ریشه‌های n م واحد در K تعریف می‌کند. درنتیجه، $\mathrm{Aut}_K F$ یک گروه دوری است که مرتبه‌اش d، n را عاد می‌کند (قضیهٔ I ۵.۳.۰ و نتیجهٔ I ۶.۴.۰). از اینرو، F روی K دوری از درجهٔ d است.

(سه) $\Rightarrow$ (یک) طبق فرض، $\mathrm{Aut}_K F$ دوری از مرتبهٔ $d = [F:K]$ با مولد σ است. فرض کنیم $\eta = \zeta^{n/d} \in K$ یک ریشهٔ d ام اولیهٔ واحد باشد. چون $N_K^F(\eta) = \eta^{[F:K]} = \eta^d = 1_K$، قضیهٔ ۶.۷ (دو) ایجاب می‌کند که به‌ازای $w \in F$ ای، $\eta = w\sigma(w)^{-1}$. هرگاه $v = w^{-1}$، آنگاه $\sigma(v) = \eta v$ و $\sigma(v^d) = (\eta v)^d = \eta^d v^d = v^d$. چون F روی K گالوا است، $v^d = b$ باید در K باشد؛ درنتیجه، v ریشه‌ای از $x^d - b \in K[x]$ می‌باشد. بنابر لم ۱۰.۷، $K(v) \subset F$ و $K(v)$ یک میدان تجزیه‌گر $x^d - b$ روی K است (که ریشه‌های متمایز آن عبارتند از $v, \eta v, \ldots, \eta^{d-1} v$). به‌علاوه، به‌ازای هر i $(0 \le i \le d-1)$؛ $\sigma^i(v) = \eta^i v$؛ درنتیجه، $\sigma^i : K(v) \cong K(\eta^i v)$. بنابر نتیجهٔ ۹.۱، v و $\eta^i v$ ریشه‌های یک چندجمله‌ای تحویل‌ناپذیر روی K اند. درنتیجه، $x^d - b$ در $K[x]$ تحویل‌ناپذیر است. بنابراین، $[K(v):K] = d = [F:K]$، که از آنجا $F = K(v)$.

(دو) $\Rightarrow$ (سه) هرگاه $v \in F$ ریشه‌ای از $x^d - b \in K[x]$ باشد، آنگاه، طبق لم ۱۰.۷، $F = K(v)$. اما $(\zeta v)^n = \zeta^n v^n = 1_K v^{d(n/d)} = b^{n/d} \in K$؛ درنتیجه، ζv ریشه‌ای از $x^n - a \in K[x]$ است، که $a = b^{n/d}$. مجددا "بنابرلم ۱۰.۷، $K(\zeta v)$ یک میدان تجزیه‌گر $x^n - a$ روی K است. اما K $\zeta \in K$ ایجاب می‌کند که $F = K(v) = K(\zeta v)$.

واضح است که ریشه‌های n م اولیهٔ واحد نقش مهمی در اثبات نتایج پیشگفته دارند. توصیف میدانهای تجزیه‌گر چندجمله‌ایها به شکل $x^n - a \in K[x]$، وقتی K شامل یک ریشهٔ n م اولیهٔ واحد نباشد، خیلی مشکلتر است. حالت $a = 1_K$ در بخش ۸ مطرح خواهد شد.

تمرینات

۱. هرگاه در تعریف ۱۰.۷ $\bar{K}$ با توسیع نرمال دلخواه N از K شامل F عوض شود، آنگاه این تعریف جدید نرم و اثر با تعریف اصلی معادل است. بخصوص، تعریف جدید به انتخاب N بستگی ندارد. ر.ک. تمرین ۲۱.۳.

۲. فرض کنید F یک توسیع با بعد متناهی از میدان متناهی K باشد. نرم N_K^F و اثر T_K^F (به عنوان نگاشتهایی چون $F \to K$) سورژکتیو می‌باشند.

۳. فرض کنید $\bar{\mathbf{Q}}$ یک بست جبری (ثابت) $\mathbf{Q}$ بوده و $v \in \bar{\mathbf{Q}}$ و $v \notin \mathbf{Q}$. همچنین، E زیرمیدانی از $\bar{\mathbf{Q}}$ باشد که نسبت به شرط $v \notin E$ ماکزیمال است. ثابت کنید هر توسیع با بعد متناهی E دوری است.

۴ . فرض کنید K یک‌میدان‌بوده، $\bar{K}$ یک‌بست‌جبری K باشد، و $\sigma \in \mathrm{Aut}_K \bar{K}$. همچنین،

$$F = \{u \in \bar{K} \mid \sigma(u) = u\}.$$

در این صورت، F میدان بوده و هر توسیع با بعد متناهی F دوری است.

۵ . هرگاه F یک توسیع دوری K از درجهٔ p^n (p: اول) بوده و L یک میدان میانی باشد به‌طوری‌که $F = L(u)$ و L روی K دوری‌ازدرجهٔ p^{n-1} باشد، آنگاه $F = K(u)$.

۶ . اگر $\mathrm{char}\ K = p \neq 0$ ، قرار دهید $K_p = \{u^p - u \mid u \in K\}$.

(آ) یک توسیع میدان دوری مانند F از K از درجهٔ p وجود دارد اگر و فقط اگر $K \neq K_p$.

(ب) هرگاه یک توسیع دوری از درجهٔ p از K موجود باشد، آنگاه، به‌ازای هر $n \geq 1$ ، یک توسیع دوری از درجهٔ p^n وجود خواهد داشت. [**راهنمایی.** از استقرا استفاده‌کنید: اگر E روی K دوری‌و از درجهٔ p^{n-1} باشد و $\mathrm{Aut}_K E$ به وسیلهٔ σ تولید شود، نشان دهید که $u, v \in E$ ای وجود دارند به‌طوری‌که $T_K^E(v) = 1_K$ و $\sigma(u) - u = v^p - v$. در این صورت، $x^p - x - u \in E[x]$ تحویل‌ناپذیر است و هرگاه w یک ریشه باشد، آنگاه $K(w)$ دوری از درجهٔ p^n روی K می‌باشد.]

۷ . هرگاه n عدد صحیح فردی باشدبه طوری‌که K شامل یک ریشهٔ n م اولیهٔ واحد بوده و $\mathrm{char}\ K \neq 2$ ، آنگاه K شامل یک ریشهٔ $2n$ م اولیهٔ واحد نیز می‌باشد.

۸ . هرگاه F یک توسیع با بعد متناهی $\mathbf{Q}$ باشد، آنگاه F فقط شامل تعدادی‌متناهی ریشهٔ واحد است.

۹ . چه ریشه‌هایی از واحد در میدانهای زیر قرار دارند:

$$\mathbf{Q}(i), \mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{-2}), \mathbf{Q}(\sqrt{-3})\ ?$$

۱۰ . (آ) فرض کنید p اول بوده و (یک) $\mathrm{char}\ K = p$ یا (دو) $\mathrm{char}\ K \neq p$ و K شامل یک ریشهٔ p ام اولیهٔ واحد باشد. در این صورت، $x^p - a \in K[x]$ یا تحویل‌ناپذیر است یا در $K[x]$ تجزیه می‌شود.

(ب) هرگاه $\mathrm{char}\ K = p \neq 0$ ، آنگاه، به‌ازای هر ریشهٔ u از $x^p - a \in K[x]$ ، $K(u) \neq K(u^p)$ اگر و فقط اگر $[K(u) : K] = p$.

۸ توسیعهای دایره بر

این بخش، جزقضیهٔ ۱۰۸ ، در آینده به کار نمی‌آید. ما میدانهای تجزیه‌گر چندجمله‌ای

$x^n - 1_K$ را، با توجهی خاص به حالت $K = \mathbf{Q}$، بررسی می‌کنیم. خواهیم دید که این میدانهای تجزیه‌گر توسیعهایی آبلی‌اند که گروههای گالوای آنها مشهور می‌باشند.

میدان تجزیه‌گر F روی میدان K از $x^n - 1_K \in K[x]$ ($n \geq 1$) یک **توسیع دایره‌بر از مرتبهٔ n** نام دارد. هرگاه $\text{char } K = p \neq 0$ و $n = mp^t$ با $(p,m) = 1$، آنگاه $x^n - 1_K = (x^m - 1)^{p^t}$ (تمرین III ۱۱.۱۰)؛ درنتیجه، یک توسیع دایره‌بر از مرتبهٔ n با یک توسیع از مرتبهٔ m یکی است. لذا، معمولا" فرض می‌کنیم $\text{char } K$، n را عاد نمی‌کند (یعنی، $\text{char } K = 0$ یا نسبت به n اول است).

بعد یک توسیع میدان دایره‌بر از مرتبهٔ n به **تابع اویلر** φ در نظریهٔ مقدماتی اعداد مربوط است، که به هر عدد صحیح مثبت n تعداد $\varphi(n)$ اعداد صحیح i که $1 \leq i \leq n$ و $(i,n) = 1$ را نسبت می‌دهد. مثلا"، $\varphi(6) = 2$ و، به‌ازای هر p اول، $\varphi(p) = p - 1$. فرض کنیم $\bar{i}$ نقش $i \in \mathbf{Z}$ تحت تصویر کانونی $\mathbf{Z} \to Z_n$ باشد. به آسانی تحقیق می‌شود که $(i,n) = 1$ اگر و فقط اگر $\bar{i}$ یک یکه در حلقهٔ Z_n باشد (تمرین ۱). بنابراین، گروه ضربی یکه‌ها در Z_n دارای مرتبهٔ $\varphi(n)$ است؛ برای ساختار این گروه، ر.ک. تمرین ۴.

قضیهٔ ۱۰.۸. *فرض کنیم n عدد صحیح مثبتی بوده، K یک میدان باشد به‌طوری‌که n، $\text{char } K$ را عاد نکند، و F یک توسیع دایره‌بر K از مرتبهٔ n باشد.*

(یک) $F = K(\zeta)$، که در آن $\zeta \in F$ یک ریشهٔ n ام اولیهٔ واحد است.

(دو) F یک توسیع آبلی با بعد d است، که $d \mid \varphi(n)$ (φ تابع اویلر است)؛ اگر n اول باشد، F عملا" یک توسیع دوری می‌شود.

(سه) $Aut_K F$ با زیرگروهی از مرتبهٔ d از گروه ضربی یکه‌های Z_n یکریخت است.

چند تبصره. به یاد آورید که هر توسیع آبلی یک توسیع گالوای جبری است که گروه گالوای آن آبلی می‌باشد. بعد F روی K ممکن است اکیدا" کوچکتر از $\varphi(n)$ باشد. مثلا"، هرگاه ζ یک ریشهٔ 5 ام واحد در $\mathbf{C}$ باشد، آنگاه $\mathbf{R} \subset \mathbf{R}(\zeta) \subset \mathbf{C}$، که از آنجا $[\mathbf{R}(\zeta) : \mathbf{R}] = 2 < 4 = \varphi(5)$. هرگاه $K = \mathbf{Q}$، آنگاه ساختار گروه $\text{Aut}_{\mathbf{Q}} F$ کاملا" با تمرین ۷ معین می‌شود.

طرح برهان ۱۰۸ . (یک) تبصره‌های پیش از لم ۱۰۰۷ نشان می‌دهند که F شامل یک ریشهٔ n م اولیهٔ واحد مانند ζ است. بنابر تعریف، $1_K, \zeta, \ldots, \zeta^{n-1} \in K(\zeta)$، n ریشهٔ متمایز $x^n - 1_K$ اند، که از آنجا $F = K(\zeta)$. (دو) و (سه) چون عوامل تحویل‌ناپذیر $x^n - 1_K$ بوضوح جدایی‌پذیرند، قضیهٔ ۱۱۰۳ و تمرین ۱۳۰۳ ایجاب می‌کنند که F روی K گالوا باشد. هرگاه $\sigma \in \mathrm{Aut}_K F$، آنگاه σ کاملا" با $\sigma(\zeta)$ معین می‌شود. طبق قضیهٔ ۲۰۲، به‌ازای i ی $(1 \le i \le n-1)$، $\sigma(\zeta) = \zeta^i$. به همین نحو، $\sigma^{-1}(\zeta) = \zeta^j$ ؛ درنتیجه $\zeta = \sigma^{-1}\sigma(\zeta) = \zeta^{ij}$، بنابر قضیهٔ ۴۰۳۰ I (پنج)، $ij \equiv 1 \pmod n$ ؛ و درنتیجه، $\bar{i} \in Z_n$ یک یکه است (که تحت تصویر کانونی $i \mapsto \bar{i}$ ، $\mathbf{Z} \to Z_n$). تحقیق کنید که انتساب به‌صورت $\sigma \mapsto \bar{i}$ یک تکریختی مانند f از $\mathrm{Aut}_K F$ به‌گروه ضربی (آبلی) یکه‌های حلقهٔ Z_n (که طبق تمرین ۱ دارای مرتبهٔ $\varphi(n)$ است) تعریف می‌کند. بنابراین، $\mathrm{Aut}_K F \cong \mathrm{Im}\, f$ آبلی از مرتبهٔ d است‌که $\varphi(n)$ را عاد می‌کند. لذا، طبق قضیهٔ اساسی ۵۰۲، $[F:K] = d$. هرگاه n اول باشد، آنگاه، طبق قضیهٔ ۳۰۵، Z_n میدان بوده و $\mathrm{Aut}_K F \cong \mathrm{Im}\, f$ دوری است.

فرض کنیم n یک عدد صحیح مثبت بوده، K میدانی باشد که $\mathrm{char}\, K$، n را عاد نمی‌کند، و F یک توسیع دایره‌بر از مرتبهٔ n از K باشد. **چندجمله‌ای دایره‌بر n** م روی K چندجمله‌ای تکین $g_n(x) = (x - \zeta_1)(x - \zeta_2)\cdots(x - \zeta_r)$ است، که در آن $\zeta_1, \ldots, \zeta_r$ تمام ریشه‌های n م اولیهٔ متمایز واحد در F می‌باشند.

چند مثال . $g_1(x) = x - 1_K$ و $g_2(x) = (x - (-1_K)) = x + 1_K$. هرگاه $K = \mathbf{Q}$، آنگاه

$$g_3(x) = (x - (-1/2 + \sqrt{3}i/2))(x - (-1/2 - \sqrt{3}i/2)) = x^2 + x + 1$$

و

$$g_4(x) = (x - i)(x + i) = x^2 + 1 .$$

این امثله چند خاصیت چندجمله‌ایهای دایره‌بر را آشکار می‌سازند.

حکم ۲۰۸ . *فرض کنیم n یک عدد صحیح مثبت بوده، K میدانی باشد که $\mathrm{char}\, K$، n را عاد نکند، و $g_n(x)$ چندجمله‌ای دایره‌بر n م روی K باشد.*

(یک) $$x^n - 1_K = \prod_{d \mid n} g_d(x) .$$

(دو) ضرایب $g_n(x)$ در زیر میدان اول P از K قرار دارند. هرگاه $char\, K = 0$ و P با میدان اعداد گویای Q یکی شود، آنگاه ضرایب عملا "اعدادی صحیح‌اند.

(سه) $Deg\, g_n(x) = \varphi(n)$، که در آن φ تابع اویلر است.

برهان. (یک) فرض کنیم F یک توسیع دایره‌بر از K از مرتبهٔ n بوده و $\zeta \in F$ یک ریشهٔ n م اولیهٔ واحد باشد. لم ۱۰.۷ (اعمال شده بر F) نشان می‌دهد که، به‌ازای هر مقسوم‌علیه d از n، گروه دوری $G = \langle \zeta \rangle$ متشکل از تمام ریشه‌های n م واحد شامل تمام ریشه‌های d ام واحد است. واضح است که $\eta \in G$ یک ریشهٔ d ام اولیهٔ واحد است (که $d \mid n$) اگر و فقط اگر $|\eta| = d$. بنابراین، به‌ازای هر مقسوم‌علیه d از n، و $g_d(x) = \prod_{\substack{\eta \in G \\ |\eta| = d}} (x - \eta)$

$$x^n - 1_K = \prod_{\eta \in G} (x - \eta) = \prod_{\substack{d \\ d \mid n}} \Big(\prod_{\substack{\eta \in G \\ |\eta| = d}} (x - \eta) \Big) = \prod_{\substack{d \\ d \mid n}} g_d(x).$$

(دو) حکم اول را به استقرا بر n ثابت می‌کنیم. واضح است که $g_1(x) = x - 1_K \in P[x]$. فرض کنیم (دو) به‌ازای هر $k < n$ درست باشد و قرار می‌دهیم $f(x) = \prod_{\substack{d \mid n \\ d < n}} g_d(x)$. در این صورت، طبق فرض استقرا، $f \in P[x]$ و، طبق قسمت (یک)، در $F[x]$، $x^n - 1_K = f(x)g_n(x)$. از آن سو، $x^n - 1_K \in P[x]$ و f تکین است. درنتیجه، الگوریتم تقسیم در $P[x]$ ایجاب می‌کند که به‌ازای $h, r \in P[x] \subset F[x]$ ی، $x^n - 1_K = fh + r$. بنابراین، طبق یکتایی خارج‌قسمت و باقیمانده (الگوریتم تقسیم به کار رفته در $F[x]$) باید داشته باشیم $r = 0$ و $g_n(x) = h \in P[x]$. این استقرا را تمام می‌کند. هرگاه $\text{char } K = 0$ و $P = \mathbf{Q}$، آنگاه یک استدلال استقرایی مشابه با استفاده از الگوریتم تقسیم در $\mathbf{Z}[x]$ و $\mathbf{Q}[x]$ (به جای $P[x], F[x]$) نشان می‌دهد که $g_n(x) \in \mathbf{Z}[x]$.

(سه) واضح است که $\deg g_n$ تعداد ریشه‌های n م اولیهٔ واحد است. فرض کنیم ζ یک چنین ریشهٔ اولیه باشد. درنتیجه، هر ریشهٔ (اولیهٔ) دیگر توانی از ζ است. پس، طبق قضیهٔ ۶.۳.۱، ζ^i $(1 \le i \le n)$ یک ریشهٔ n م اولیهٔ واحد است (یعنی، یک مولد G) اگر و فقط اگر $(i,n) = 1$. اما، طبق تعریف، تعداد این‌گونه i ها درست مساوی $\varphi(n)$ است.

چند تبصره. قسمت (یک) قضیه یک روش بازگشتی برای تعیین $g_n(x)$ به دست می‌دهد، زیرا

$$g_n(x) = \frac{x^n - 1_K}{\prod\limits_{\substack{d \\ d|n \\ d<n}} g_d(x)}.$$

مثلاً، هرگاه p اول باشد، آنگاه

$$g_p(x) = (x^p - 1_K)/g_1(x) = (x^p - 1_K)/(x - 1_K) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1_K.$$

با استفاده از مثال پیش از قضیهٔ ۲۰۸، به‌ازای $K = \mathbf{Q}$ داریم

$$\begin{aligned} g_6(x) &= (x^6 - 1)/g_1(x)g_2(x)g_3(x) \\ &= (x^6 - 1)/(x - 1)(x + 1)(x^2 + x + 1) \\ &= x^2 - x + 1; \end{aligned}$$

به همین نحو،

$$\begin{aligned} g_{12}(x) &= (x^{12} - 1)/(x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1) \\ &= x^4 - x^2 + 1. \end{aligned}$$

وقتی میدان پایه میدان $\mathbf{Q}$ باشد، می‌توان نتایج پیشگفته را به نحوی قوت بخشید.

حکم ۳۰۸. *فرض کنیم F یک توسیع دایره‌برای مرتبهٔ n از میدان اعداد گویای $\mathbf{Q}$ بوده و $g_n(x)$ چندجمله‌ای دایره‌بر n م روی $\mathbf{Q}$ باشد. در این صورت،*

(یک) $g_n(x)$ در $\mathbf{Q}[x]$ تحویل‌ناپذیر است؛

(دو) $[F : \mathbf{Q}] = \varphi(n)$، که در آن φ تابع اویلر است؛

(سه) $Aut_{\mathbf{Q}}F$ با گروه ضربی یکه‌ها در حلقهٔ $\mathbf{Z}_n$ یکریخت است.

طرح برهان. (یک) بنابر لم III ۱۳۰۶۰، کافی است نشان دهیم که چندجمله‌ای تکین $g_n(x)$ در $\mathbf{Z}[x]$ تحویل‌ناپذیر است. فرض کنیم h یک عامل تحویل‌ناپذیر از g_n در $\mathbf{Z}[x]$ باشد که $\deg h \geq 1$. پس $g_n(x) = f(x)h(x)$، که در آن $f, h \in \mathbf{Z}[x]$ لزوماً تکین هستند. فرض کنیم ζ ریشه‌ای از h بوده و p عدد صحیح اولی باشد که $(p,n) = 1$.

ابتدا نشان می‌دهیم که ζ^p نیز ریشه‌ای از h است. چون ζ ریشه‌ای از $g_n(x)$ است،

ζ یک ریشهٔ n م اولیهٔ واحد می‌باشد. برهان حکم ۲۰۸ (سه) ایجاب می‌کند که ζ^p نیز یک ریشهٔ n م اولیهٔ واحد، و لذا یک ریشهٔ f یا h، می‌باشد. فرض کنیم ζ^p یک ریشهٔ h نباشد. پس ζ^p ریشه‌ای از $f(x) = \sum_{i=0}^{r} a_i x^i$ است؛ و درنتیجه، ζ ریشه‌ای از $f(x^p) = \sum_{i=0}^{r} a_i x^{ip}$ است. چون h در $\mathbf{Q}[x]$ تحویل‌ناپذیر است (لم III ۱۳۰۶۰) و ζ را به عنوان ریشه دارد، بنابر قضیهٔ ۶۰۱، h باید $f(x^p)$ را عاد کند؛ مثلاً "$f(x^p) = h(x)k(x)$، که در آن $k \in \mathbf{Q}[x]$. بنابر الگوریتم تقسیم در $\mathbf{Z}[x]$، $k_1, r_1 \in \mathbf{Z}[x]$، که در آن $f(x^p) = h(x)k_1(x) + r_1(x)$. حکم یکتایی الگوریتم تقسیم در $\mathbf{Q}[x]$ نشان می‌دهد که $k(x) = k_1(x) \in \mathbf{Z}[x]$. به یاد آورید که تصویر کانونی $\mathbf{Z} \to Z_p$ (که روی عنصرها با $b \mapsto \bar{b}$ نموده می‌شود) یک بروریختی حلقه‌ها مانند $\mathbf{Z}[x] \to Z_p[x]$ با تعریف $g = \sum_{i=0}^{t} b_i x^i \mapsto \bar{g} = \sum_{i=0}^{t} \bar{b}_i x^i$ القا می‌کند (تمرین III ۱۰۵۰). درنتیجه، در $Z_p[x]$، $\bar{f}(x^p) = \bar{h}(x)\bar{k}(x)$. اما در $Z_p[x]$، $\bar{f}(x^p) = \bar{f}(x)^p$ (زیرا $\operatorname{char} Z_p = p$). بنابراین،

$$\bar{f}(x)^p = \bar{h}(x)\bar{k}(x) \in Z_p[x].$$

درنتیجه، عامل تحویل‌ناپذیری از $\bar{h}(x)$ با درجهٔ مثبت باید $\bar{f}(x)^p$، و درنتیجه $\bar{f}(x)$ در $Z_p[x]$، را عاد کند. از آن سو، چون $g_n(x)$ عاملی از $x^n - 1$ است، به‌ازای $r(x) \in \mathbf{Z}[x]$ ی، $x^n - 1 = g_n(x)r(x) = f(x)h(x)r(x)$. لذا، در $Z_p[x]$،

$$x^n - \bar{1} = \overline{x^n - 1} = \bar{f}(x)\bar{h}(x)\bar{r}(x).$$

چون $\bar{f}$ و $\bar{h}$ عامل مشترک دارند، $x^n - \bar{1} \in Z_p[x]$ باید ریشهٔ چندگانه داشته باشد. این امر با متمایز بودن تمام ریشه‌های $x^n - \bar{1}$ متناقض است، زیرا $(p,n) = 1$ (ر.ک. تبصره‌های پیش از لم ۱۰۰۷). بنابراین، ζ^p ریشه‌ای از $h(x)$ است.

هرگاه $r \in \mathbf{Z}$ چنان باشد که $1 \le r \le n$ و $(r,n) = 1$، آنگاه $r = p_1^{k_1} \cdots p_s^{k_s}$ که در آن $k_i > 0$ و هر p_i یک اول است که $(p_i, n) = 1$. کاربرد مکرر این امر که ζ^p ریشه‌ای از h است هر وقت ζ چنین باشد نشان می‌دهد که ζ^r ریشه‌ای از $h(x)$ است. اما، بنابر برهان حکم ۲۰۸ (سه)، ζ^r ها ($1 \le r \le n$ و $(r,n) = 1$) دقیقاً "تمام ریشه‌های n م اولیهٔ واحد می‌باشند. لذا، $h(x)$ بر $g_n(x) = \prod_{\substack{1 \le r \le n \\ (r,n)=1}} (x - \zeta^r)$ بخشپذیر است، که از آنجا $g_n(x) = h(x)$.

بنابراین، $g_n(x)$ تحویل‌ناپذیر است.

(دو) لم ۱۰۰۷ نشان‌می‌دهدکه $F = \mathbf{Q}(\zeta)$ ، که ازآنجا ،طبق‌حکم ۲۰۸ و قسمت (یک) ،

$$[F : \mathbf{Q}] = [\mathbf{Q}(\zeta) : \mathbf{Q}] = \deg g_n = \varphi(n) .$$

قسمت (سه) نتیجه‌ای است از قسمت (دو) ، قضیهٔ ۱۰۸ ، وتمرین ۱ .

تبصره. قضیهٔ نابدیهی کرونکر می‌گوید که هر توسیع آبلی $\mathbf{Q}$ مشمول یک توسیع دایره‌بر است .

تمرینات

۱ . اگر $i \in \mathbf{Z}$ ، $\bar{i}$ نقش i تحت تصویرکانونی $\mathbf{Z} \to Z_n$ در Z_n است. ثابت کنید $\bar{i}$ در حلقهٔ Z_n یکه است اگر و فقط اگر $(i,n) = 1$. بنابراین ، گروه ضربی یکه‌ها در Z_n از مرتبهٔ $\varphi(n)$ می‌باشد .

۲ . خواص تابع اویلر φ مذکور در زیر را ثابت کنید .

(آ) هرگاه p اول بوده و $n > 0$ ، آنگاه $\varphi(p^n) = p^n(1 - 1/p) = p^{n-1}(p - 1)$.

(ب) هرگاه $(m,n) = 1$ ، آنگاه $\varphi(mn) = \varphi(m)\varphi(n)$.

(پ) هرگاه $n = p_1^{k_1} \cdots p_r^{k_r}$ (p_i ها اول و متمایزند ؛ $k_i > 0$) ، آنگاه

$$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_r) .$$

(ت) $\sum_{d|n} \varphi(d) = n$.

(ث) $\varphi(n) = \sum_{d|n} d\mu(n/d)$ ، که در آن μ تابع موبیوس[1] است که به‌صورت زیر تعریف می‌شود :

$$\mu(n) = \begin{cases} 1 & \text{اگر } n = 1 \text{ ،} \\ (-1)^t & \text{اگر } n \text{ حاصلضربی از } t \text{ اول متمایز باشد ،} \\ 0 & \text{اگر به‌ازای اولی چون } p \text{ ، } p^2 \text{ ، } n \text{ را عاد کند ،} \end{cases}$$

۳ . فرض کنید φ تابع اویلر باشد .

(آ) به‌ازای $n > 2$ ، $\varphi(n)$ زوج است .

(ب) تمام $n > 0$ هایی را بیابید که $\varphi(n) = 2$.

(پ) تمام جفتهای (n,p) (که $n,p > 0$ و p اول است) را بیابید که $\varphi(n) = n/p$.
[ر.ک. تمرین ۲ .]

1. Moebius

۴ . (آ) هرگاه p اول و فرد بوده و $n > 0$ ، آنگاه گروه ضربی یکه‌ها در حلقهٔ Z_{p^n} دوری از مرتبهٔ $p^{n-1}(p-1)$ است .

(ب) قسمت (آ) در صورتی که $p = 2$ و $n \geq 2$ نیز برقرار است .

(پ) هرگاه $n \geq 3$ ، آنگاه گروه ضربی یکه‌ها در Z_{2^n} با $Z_2 \oplus Z_{2^{n-2}}$ یکریخت است .

۵ . اگر $f(x) = \sum_{i=0}^{t} a_i x^i$ ، $f(x^s)$ را چندجمله‌ای $\sum_{i=0}^{t} a_i x^{is}$ بگیرید . خواص چندجمله‌ایهای دایره بر $g_n(x)$ روی $\mathbf{Q}$ ی مذکور در زیر را به دست آورید .

(آ) هرگاه p اول بوده و $k \geq 1$ ، آنگاه $g_{p^k}(x) = g_p(x^{p^{k-1}})$.

(ب) هرگاه $n = p_1^{r_1} \cdots p_k^{r_k}$ (p_i ها اول و متمایزند ؛ $r_i > 0$) ، آنگاه

$$g_n(x) = g_{p_1 \cdots p_k}(x^{p_1^{r_1-1} \cdots p_k^{r_k-1}}).$$

(پ) هرگاه n فرد باشد ، آنگاه $g_{2n}(x) = g_n(-x)$.

(ت) هرگاه p اول بوده و $p \nmid n$ ، آنگاه $g_{pn}(x) = g_n(x^p)/g_n(x)$.

(ث) $g_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$ ، که در آن μ تابع موبیوس تمرین ۲ (ث) است .

(ج) $g_n(1) = p$ اگر $n = p^k$ $(k > 0)$ ، 0 اگر $n = 1$ ، و 1 در غیراین صورت .

۶ . چندجمله‌ایهای دایره‌بر n م روی $\mathbf{Q}$ ی تمام n های مثبت که $n \leq 20$ را حساب کنید .

۷ . فرض کنید F_n یک توسیع دایره‌بر $\mathbf{Q}$ از مرتبهٔ n باشد . ساختار $\mathrm{Aut}_{\mathbf{Q}}F_n$ را به‌ازای هر n تعیین کنید . [**راهنمایی .** هرگاه U_n^* گروه ضربی یکه‌ها در Z_n باشد ، آنگاه نشان دهید $U_n^* = \prod_{i=1}^{r} U_{p_i^{n_i}}^*$ ، که در آن n دارای تجزیه به عوامل اول $n = p_1^{n_1} \cdots p_r^{n_r}$ می‌باشد . تمرین ۴ را به کار برید .]

۸ . فرض کنید F_n یک توسیع دایره‌بر $\mathbf{Q}$ از مرتبهٔ n باشد .

(آ) $\mathrm{Aut}_{\mathbf{Q}}F_8$ و تمام میدانهای میانی را تعیین کنید .

(ب) همین کار را برای F_8 انجام دهید .

(پ) همین کار را برای F_7 انجام دهید ؛ اگر ζ یک ریشهٔ 7 م اولیهٔ واحد باشد ، چندجمله‌ای تحویل‌ناپذیر $\zeta + \zeta^{-1}$ روی $\mathbf{Q}$ چیست ؟

۹ . هرگاه $n > 2$ و ζ یک ریشهٔ n م اولیهٔ واحد روی $\mathbf{Q}$ باشد ، آنگاه

$$[\mathbf{Q}(\zeta + \zeta^{-1}) : \mathbf{Q}] = \varphi(n)/2$$

۱۰ . (ودر بورن[1]) هرحلقهٔ بخشی متناهی D یک میدان است . در اینجا برهان کوتاهی ازآن عرضه می‌شود (که‌درآن E^* گروه ضربی عناصر ناصفر حلقهٔ بخشی E است) .

(آ) مرکز K از D یک میـدان و D یک فضای بـرداری روی K است ، که از آنجا $|D| = q^n$ که $q = |K| \geq 2$.

(ب) هرگاه $0 \neq a \in D$ ، آنگاه $N(a) = \{d \in D \mid da = ad\}$ یک حلقهٔ زیر بخشی D شامل K است . به علاوه ، $|N(a)| = q^r$ ، که در آن $r \mid n$.

(پ) هرگاه $0 \neq a \in D - K$ ، آنگاه $N(a)^*$ مرکزسار a درگروه D^* بوده‌و ، به‌ازای r ی که $1 \leq r < n$ و $r \mid n$ ، $[D^* : N(a)^*] = (q^n - 1)/(q^r - 1)$.

(ت) $q^n - 1 = q - 1 + \sum_r (q^n - 1)/(q^r - 1)$ ، که‌درآن مجموع آخر روی تعدادی متناهی عدد صحیح مانند r گرفته می‌شود که $1 \leq r < n$ و $r \mid n$.

[**راهنمایی .** از معادلهٔ رده‌ای D^* استفاده کنیـد ؛ ر.ک. صفحات ۱۴۰ تا ۱۴۱ .]

(ث) به‌ازای هر ریشهٔ n م اولیهٔ واحد مانند $\zeta \in \mathbf{C}$ ، $|q - \zeta| > q - 1$ ، که در آن به‌ازای $a + bi \in \mathbf{C}$ ، $|a + bi| = \sqrt{a^2 + b^2}$. درنتیجه ، $|g_n(q)| > q - 1$ ، که در آن g_n چندجمله‌ای دایره‌بر n م روی $\mathbf{Q}$ است .

(ج) معادلـهٔ مذکوردر (ت) غیرممکن‌است مگرآنکه $n = 1$ ، که ازآنجا $K = D$.

[**راهنمایی .** از حکـم ۲۰۸ استفاده کـرده ، نشان‌دهید که به‌ازای هر مقسوم‌علیه مثبت r از n که $r \neq n$ ، $f_r(x) = (x^n - 1)/(x^r - 1)$ در $\mathbf{Z}[x]$ بـوده و ، بـه‌ازای $h_r(x) \in \mathbf{Z}[x]$ ی $f_r(x) = g_n(x)h_r(x)$. درنتیجه ، بـه‌ازای هر r ، $g_n(q)$ ، $f_r(q)$ را در $\mathbf{Z}$ عاد می‌کند ، که از آنجا ، بنابر (ت) ، $g_n(q) \mid (q - 1)$. این قسمت (ث) را نقض خواهد کرد .]

۹ توسیعهای رادیکالی

ریشهٔ تاریخی نظریهٔ گالوا در یک مسئلهٔ کلاسیک در نظریهٔ معادلات است ، که می‌توان آن را شهودا" ولی به‌طور معقول به صورت دقیق زیر بیان کرد . اگر میدان K داده شده باشد ، آیا یک "فرمول" صریح (مستلزم فقط اعمال میدان و ریشهٔ n م گیری) وجود دارد که تمام جوابهای معادلهٔ چندجمله‌ای $(f \in K[x])$ $f(x) = 0$ *دلخواه* را بـه ما بدهد ؟ اگر

1.Wedderlurn

درجهٔ f حداکثر چهار باشد، جواب مثبت است (مثلا"، "فرمول درجهٔ دوم" آشنا وقتی $\deg f = 2$ و $\text{char } K \neq 2$. همچنین، ر.ک. تمرین ۵) . با اینحال، نشان می‌دهیم که جواب درحالت کلی منفی‌است (حکم ۸.۹) . برای این کار بعضی از توسیعهای میدان را توصیف می‌کنیم که گروههای گالوای آنها حلپذیرند (قضیهٔ ۴.۹ و حکم ۶.۹) .

اولین کار تنظیم صورت دقیق مسئلهٔ کلاسیک با اصطلاحات نظریهٔ میدانهاست . در سراسر بحث در یک بست جبری ثابت میدان پایهٔ داده شدهٔ K کار خواهیم کرد . شهودا" ، وجود یک "فرمول" برای حل یک معادلهٔ چندجمله‌ای **معین** $f(x) = 0$ یعنی دنباله‌ای متناهی از مراحل وجود دارد که هر کدام یک عمل میدان (جمع ، ضرب ، معکوس‌گیری) یا ریشهٔ n م گرفتن است ، که تمام جوابهای معادلهٔ داده شده را به ما می‌دهد . انجام یک عمل میدان ، میدان پایه را تغییر نمی‌دهد ، ولی ریشهٔ n م‌گیری از عنصر c در میدان E منجر به ساختن یک توسیع میدان مانند $E(u)$ می‌شود که $u^n \in E$ (یعنی ، $u = \sqrt[n]{c}$) . لذا ، وجود یک "فرمول" برای حل $f(x) = 0$ درواقع وجود یک زنجیر متناهی مانند

$$K = E_0 \subset E_1 \subset \cdots \subset E_n$$

از میدانها را ایجاب می‌کند که E_n شامل یک میدان تجزیه‌گر از f روی K بوده و ، به‌ازای هر $i \geq 1$ ، $E_i = E_{i-1}(u_i)$ که توان مثبتی از u_i در E_{i-1} قرار دارد .

به عکس، فرض کنیم چنین زنجیری از میدانها وجود داشته و E_n شامل میدان تجزیه‌گری از f باشد (یعنی ، E_n شامل تمام جوابهای $f(x) = 0$ است) . در این صورت ،

$$E_n = K(u_1, \ldots, u_n)$$

و ، بنابر قضیهٔ ۳.۱ ، هرجواب به شکل زیر است:

$$f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) \qquad (f, g \in K[x_1, \ldots, x_n]).$$

لذا ، هر جواب را می‌توان برحسب تعدادی متناهی عنصر K ، تعدادی‌متناهی اعمال میدان ، و $u_1, \ldots, u_n$ (که با ریشه‌گیری به دست می‌آیند) بیان کرد . اما این معادل آن است که بگوییم یک "فرمول" برای جوابهای معادلات داده شده وجود دارد . این نکات انگیزهٔ دو تعریف زیر خواهند بود .

تعریف ۱.۹ . توسیع میدان F از میدان K یک **توسیع رادیکالی** K است اگر $F = K(u_1, \ldots, u_n)$ ، توانی از u_1 در K واقع باشد و ، به‌ازای هر $i \geq 2$ ، توانی از u_i

در $K(u_1, \ldots, u_{i-1})$ واقع باشد.

چند تبصره. هرگاه $u_i^m \in K(u_1, \ldots, u_{i-1})$ ، آنگاه u_i ریشه‌ای از

$$x^m - u_i^m \in K(u_1, \ldots, u_{i-1})[x]$$

است. از اینرو، بنابر قضیهٔ ۱۲۰۱ ، $K(u_1, \ldots, u_i)$ روی $K(u_1, \ldots, u_{i-1})$ جبری با بعد متناهی است. بنابراین، طبق قضایای ۲۰۱ و ۱۱۰۱ ، هر توسیع رادیکالی F از K روی K جبری و با بعد متناهی می‌باشد.

تعریف ۲۰۹ . فرض‌کنیم K میدان بوده و $f \in K[x]$. معادلهٔ $f(x) = 0$ ***حلپذیر به‌وسیلهٔ رادیکالها*** است اگر یک توسیع رادیکالی مانند F از K و یک میدان تجزیه‌گر مانند E از f روی K موجود باشد به‌طوری‌که $F \supset E \supset K$.

تعریف ۲۰۹ اولین گام در تنظیم مسئلهٔ کلاسیک یافتن یک "فرمول" برای جوابهای $f(x) = 0$ است که **برای هر** چندجمله‌ای $f \in K[x]$ از درجهٔ معلوم r (مانند فرمول درجهٔ دوم به‌ازای $r = 2$) معتبرباشد. تعریف دقیق یک چنین "فرمول" هرچه باشد، از بحث پیش از تعریف ۱۰۹ روشن است که‌وجود چنین "فرمول" باید ایجاب کند که هر معادلهٔ چندجمله‌ای از درجهٔ r حلپذیر به وسیلهٔ رادیکالها باشد.

لذا، برای نشان دادن عدم وجود چنین فرمول، کافی است ثابت کنیم یک معادلهٔ چندجمله‌ای خاص حلپذیر به وسیلهٔ رادیکالها نیست. حال معلومات لازم برای این کار را کسب کرده (نتیجهٔ ۵۰۹) و تنظیم دقیق مسئلهٔ کلاسیک را به‌ضمیمه وامی‌گذاریم.

لم ۳۰۹ . *هرگاه F یک توسیع میدان رادیکالی K و N یک بست نرمال F روی K باشد (قضیهٔ ۱۶۰۳)، آنگاه N یک توسیع رادیکالی K است.*

طرح برهان. برهان مرکب از تلفیق دو امر است. (یک) هرگاه F یک توسیع با بعد متناهی K (نه‌لزوما "رادیکالی") بوده و N بست نرمال F روی K باشد، آنگاه N میدان مرکب $E_1E_2 \cdots E_r$ است، که در آن هر E_i زیرمیدانی از N است که با F ، K ــ یکریخت است. (دو) هرگاه هر یک از $E_1, \ldots, E_r$ توسیع رادیکالی از K باشد (که در اینجا

چنین‌است، زیرا F رادیکالی است)، آنگاه میدان مرکب $E_1E_2\cdots E_r$ یک توسیع رادیکالی K می‌باشد. این احکام به‌صورت زیر توجیه می‌شوند.

(یک) فرض کنیم $\{w_1,\ldots,w_n\}$ پایه‌ای‌از F روی K بوده‌و f_i چندجمله‌ای تحویل‌ناپذیر از w_i روی K باشد. برهان قضیهٔ ۱۶۰۳ نشان می‌دهد که N یک میدان تجزیه‌گر $\{f_1,\ldots,f_n\}$ روی K است. فرض کنیم v ریشه‌ای از f_i در N باشد. در این صورت، بنابر قضیهٔ ۸۰۱، یک K ــ یکریختی مانند $\sigma : K(w_i)\cong K(v)$ وجود دارد به‌طوری‌که $\sigma(w_i)=v$. بنابر قضیهٔ ۸۰۳، σ به K ــ خودریختی τ از N توسیع می‌یابد. واضح است که $\tau(F)$ زیرمیدانی‌از N است‌که‌با K، F ــ یکریخت‌بوده‌وشامل $\tau(w_i)=\sigma(w_i)=v$ می‌باشد. بدین ترتیب، می‌توان به‌ازای هر ریشهٔ v و هر f_i یک زیرمیدان مانند E از N یافت که $v\in E$ و E با F، K ــ یکریخت می‌باشد. هرگاه $E_1,\ldots,E_r$ زیرمیدانهایی باشند که این‌طور به‌دست می‌آیند، آنگاه $E_1E_2\cdots E_r$ زیرمیدانی از N است که شامل تمام ریشه‌های $f_1,f_2,\ldots,f_n$ است، که از آنجا $E_1E_2\cdots E_r=N$.

(دو) فرض کنیم، همانند در تعریف ۱۰۹، $r=2$، $E_1=K(u_1,\ldots,u_k)$، و $E_2=K(v_1,\ldots,v_m)$. در این صورت، $E_1E_2=K(u_1,\ldots,u_k,v_1,\ldots,v_m)$ بوضوح یک‌توسیع رادیکالی K است. حالت کلی به همین نحو خواهد بود.

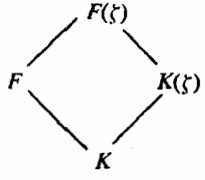
قضیهٔ ۴۰۹. *هرگاه F یک توسیع میدان رادیکالی از K و E یک میدان میانی باشد، آنگاه $\mathrm{Aut}_K E$ یک گروه حلپذیر است.*

برهان. هرگاه K_0 میدان ثابت E نسبت‌به‌گروه $\mathrm{Aut}_K E$ باشد، آنگاه E روی K_0 گالواست، $\mathrm{Aut}_{K_0}E=\mathrm{Aut}_K E$، و F یک توسیع رادیکالی K_0 است (تمرین ۱). لذا، می‌توان با این فرض شروع کرد که E روی K گالوای جبری است. فرض کنیم N یک بست نرمال F روی K باشد (قضیهٔ ۱۶۰۳). در این صورت، طبق لم ۳۰۹، N یک توسیع رادیکالی K بوده و، بنابرلم ۱۳۰۲، E یک میدان‌میانی پایداراست. درنتیجه، تحدید $(\sigma\mapsto\sigma\mid E)$ یک همریختی مانند $\theta:\mathrm{Aut}_K N\to\mathrm{Aut}_K E$ القا خواهد کرد. چون N یک میدان تجزیه‌گر روی K (و درنتیجه، روی E) است، بنابر قضیهٔ ۸۰۳، هر $\sigma\in\mathrm{Aut}_K E$ به یک K ــ خودریختی N توسیع می‌یابد. بنابراین، θ یک‌بروریختی‌است. چون نقش‌همریخت یک گروه حلپذیراست (قضیهٔ II ۱۱۰۷۰)، کافی است ثابت کنیم $\mathrm{Aut}_K N$ حلپذیر است.

هرگاه K_1 میدان ثابت N نسبت به $\mathrm{Aut}_K N$ باشد، آنگاه N یک توسیع گالوای رادیکالی K_1 بوده (تمرین ۱) و $\mathrm{Aut}_{K_1} N = \mathrm{Aut}_K N$. بنابراین، می‌توان به نمادهای اصلی خود بازگشت و بدون لطمه زدن به کلیت فرض کرد $F = E$ و F یک توسیع گالوای رادیکالی از K باشد.

هرگاه $F = K(u_1, \ldots, u_n)$ که در آن $u_1^{m_1} \in K$ و، به‌ازای $i \geq 2$، $u_i^{m_i} \in K(u_1, \ldots, u_{i-1})$، آنگاه می‌توان فرض کرد که m_i، $\mathrm{char}\, K$ را عاد نمی‌کند. این در صورتی که $\mathrm{char}\, K = 0$ واضح است. هرگاه $\mathrm{char}\, K = p \neq 0$ و $m_i = rp^t$ که $(r,p) = 1$، آنگاه $u_i^{rp^t} \in K(u_1, \ldots, u_{i-1})$؛ درنتیجه، u_i^r روی $K(u_1, \ldots, u_{i-1})$ صرفاً "جدایی‌ناپذیر است. اما F روی K گالوا، و لذا جدایی‌پذیر، است (قضیهٔ ۱۱.۳)، که از آنجا F روی $K(u_1, \ldots, u_{i-1})$ جدایی‌پذیر است (تمرین ۱۲.۳). بنابراین، طبق قضیهٔ ۲.۶، $u_i^r \in K(u_1, \ldots, u_{i-1})$، و می‌توان فرض کرد $m_i = r$.

هرگاه $\mathrm{char}\, K\,(= \mathrm{char}\, F)$، $m = m_1 m_2 \cdots m_n$، آنگاه، بنابر بند پیشین، m را عاد نمی‌کند. توسیع دایره‌بر $F(\zeta)$ از F را درنظر می‌گیریم، که در آن ζ یک ریشهٔ m م اولیهٔ واحد است (قضیهٔ ۱.۸). وضع به صورت زیر است:



که در آن $F(\zeta)$ روی F گالوا است (قضیهٔ ۱.۸)؛ و درنتیجه، روی K نیز چنین است (تمرین ۱۵.۳ (ب)). قضیهٔ اساسی ۵.۲ نشان می‌دهد که $\mathrm{Aut}_K F \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_F F(\zeta)$. درنتیجه، بنابر قضیهٔ II ۱۱.۷۰، کافی است ثابت کنیم $\mathrm{Aut}_K F(\zeta)$ حلپذیر است. توجه کنید که $K(\zeta)$ یک توسیع گالوای آبلی K است (قضیهٔ ۱.۸)، که از آنجا، بنابر قضیهٔ اساسی ۵.۲، $\mathrm{Aut}_K K(\zeta) \cong \mathrm{Aut}_K F(\zeta)/\mathrm{Aut}_{K(\zeta)} F(\zeta)$. هرگاه می‌دانستیم که $\mathrm{Aut}_{K(\zeta)} F(\zeta)$ حلپذیر است، آنگاه قضیهٔ II ۱۱.۷ ایجاب می‌کرد که $\mathrm{Aut}_K F(\zeta)$ حلپذیر است (زیرا $\mathrm{Aut}_K K(\zeta)$ آبلی، درنتیجه حلپذیر، است). لذا، کافی است ثابت کنیم $\mathrm{Aut}_{K(\zeta)} F(\zeta)$ حلپذیر است.

طبق فرض، $F(\zeta)$ روی K'، و درنتیجه روی هر میدان میانی، گالوا است. فرض کنیم $E_0 = K(\zeta)$ و

$$E_i = K(\zeta, u_1, \ldots, u_i) \qquad (i = 1,2,\ldots,n)$$

درنتیجه ، $E_n = K(\zeta, u_1, \ldots, u_n) = F(\zeta)$. فرض کنیم $H_i = \mathrm{Aut}_{E_i}F(\zeta)$ زیرگروه نظیر از $\mathrm{Aut}_{K(\zeta)}F(\zeta)$ تحت تناظر گالوا باشد . به‌طور تصویری داریم

$$\begin{array}{ccc} F(\zeta) = E_n & \longmapsto & H_n = 1 \\ \vdots & & \vdots \\ E_i & \longmapsto & H_i = \mathrm{Aut}_{E_i}F(\zeta) \\ \cup & & \\ E_{i-1} & \longmapsto & H_{i-1} = \mathrm{Aut}_{E_{i-1}}F(\zeta) \\ \vdots & & \vdots \\ K(\zeta) = E_0 & \longmapsto & H_0 = \mathrm{Aut}_{K(\zeta)}F(\zeta) \end{array}$$

بنابر لم ۱۰۰۷ (یک) ، به‌ازای هر i $(i = 1,2,\ldots,n)$ ، $K(\zeta)$ شامل یک ریشهٔ m_i م اولیهٔ واحد است . چون $E_i = E_{i-1}(u_i)$ و $u_i^{m_i} \in E_{i-1}$ ، بنابر لم ۱۰۰۷ (دو) (به‌ازای $d = m_i$) و قضیهٔ ۱۱۰۷ (دو) (به‌ازای $n = m_i$) ، هر E_i یک توسیع دوری E_{i-1} است . بخصوص، E_i روی E_{i-1} گالواست . قضیهٔ اساسی ۵۰۲ ایجاب می‌کند که به‌ازای هر $i = 1,2,\ldots,n$ ، $H_i \lhd H_{i-1}$ و $H_{i-1}/H_i \cong \mathrm{Aut}_{E_{i-1}}E_i$ ، که از آنجا H_{i-1}/H_i آبلی دوری است . درنتیجه ،

$$1 = H_n < H_{n-1} < \cdots < H_0 = \mathrm{Aut}_{K(\zeta)}F(\zeta)$$

یک سری حلپذیر است (تعریف II ۳۰۸۰) . بنابراین ، طبق قضیهٔ II ۵۰۸۰ ، $\mathrm{Aut}_{K(\zeta)}F(\zeta)$ حلپذیر است .

نتیجهٔ ۵۰۹ . *فرض کنیم K میدان بوده و $f \in K[x]$. هرگاه معادلهٔ $f(x) = 0$ حلپذیر به وسیلهٔ رادیکالها باشد ، آنگاه گروه گالوای f یک گروه حلپذیر است .*

برهان . این فورا " از قضیهٔ ۴۰۹ و تعریف ۲۰۹ به دست می‌آید .

مثال . چندجمله‌ای $f = x^5 - 4x + 2 \in \mathbf{Q}[x]$ دارای گروه گالوای S_5 است (ر.ک. مثال بعد از قضیهٔ ۱۲۰۴) ، که یک گروه حلپذیر نیست (نتیجهٔ II ۱۲۰۷۰) . بنابراین ، $x^5 - 4x + 2 = 0$ حلپذیر به وسیلهٔ رادیکالها نیست و "فرمولی" (مستلزم فقط اعمال

میدان و ریشه‌گیری) برای جوابهای آن وجود ندارد.

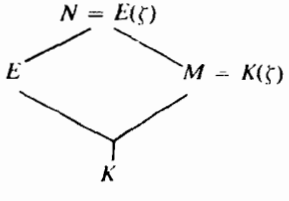
توجه کنید که دراینجا میدان‌پایه نقش مهمی دارد. چندجمله‌ای $x^5 - 4x + 2 = 0$ حلپذیر به‌وسیلهٔ رادیکالها روی $\mathbf{Q}$ نیست، ولی روی میدان اعداد حقیقی $\mathbf{R}$ حلپذیر به وسیلهٔ رادیکالهاست. درواقع، هر معادلهٔ چندجمله‌ای روی $\mathbf{R}$ حلپذیر به وسیلهٔ رادیکالهاست، زیرا تمام جوابها در بست جبری $\mathbf{C} = \mathbf{R}(i)$، که یک توسیع رادیکالی $\mathbf{R}$ است، قرار دارند.

این بخش را با اثبات عکس ناقصی از قضیهٔ ۴۰۹ به پایان می‌بریم. اگر K با مشخص صفر باشد، مشکلی وجود ندارد. اما اگر $\mathrm{char}\, K$ مثبت باشد، لازم است بر آن قیودی بگذاریم (یا "توسیع رادیکالی" را تعریف مجدد نماییم ــ ر.ک. تمرین ۲).

حکم ۶۰۹. *فرض کنیم E یک توسیع میدان گالوای با بعد متناهی از K با گروه گالوای حلپذیر $\mathrm{Aut}_K E$ باشد. همچنین، $\mathrm{char}\, K$، $[E:K]$ را عاد نکند. در این صورت، یک توسیع رادیکالی مانند F از K وجود دارد به‌طوری‌که $F \supset E \supset K$.*

تبصره. شرط گالوا بودن E روی K لازم است (تمرین ۳).

طرح برهان ۶۰۹. چون $\mathrm{Aut}_K E$ یک گروه حلپذیر متناهی است، بنابر حکم II ۶۰۸۰، دارای زیرگروه نرمالی با اندیس اول p مانند H است. چون E روی K گالواست، $|\mathrm{Aut}_K E| = [E:K]$ (قضیهٔ ۵۰۲)؛ درنتیجه، $\mathrm{char}\, K \nmid p$. فرض‌کنیم $N = E(\zeta)$ یک توسیع دایره‌بر از E باشد، که در آن ζ یک ریشهٔ p ام اولیهٔ واحد است (قضیهٔ ۱۰۸). فرض کنیم $M = K(\zeta)$؛ در این صورت، داریم



N روی E (قضیهٔ ۱۰۸)، و درنتیجه روی K (تمرین ۱۵۰۳ (ب))، گالوا و با بعد

متناهی است. اما واضح است که M یک توسیع رادیکالی K است. درنتیجه، (بنابر تمرین ۴) کافی است نشان دهیم یک توسیع رادیکالی از M شامل N وجود دارد.

ابتدا می‌بینیم که E یک میدان میانی پایدار از N و K است (لم ۱۳۰۲). لذا، تحدید $(\sigma \mid E)$ یک همریختی مانند $\theta : \mathrm{Aut}_M N \to \mathrm{Aut}_K E$ را القا می‌کند. هرگاه $\sigma \in \mathrm{Aut}_M N$، آنگاه $\sigma(\zeta) = \zeta$. از اینرو، اگر $\sigma \in \mathrm{Ker}\,\theta$، داریم $\sigma = 1_N$. بنابراین، θ یک تکریختی است.

حال قضیه را به استقرا بر $n = [E : K]$ ثابت می‌کنیم. حالت $n = 1$ بدیهی است. فرض کنیم قضیه برای تمام توسیعها با بعد $k < n$ درست باشد و دو حالت زیر را درنظر می‌گیریم:

(یک) $\mathrm{Aut}_M N$ تحت θ با زیرگروهی حقیقی از $\mathrm{Aut}_K E$ یکریخت است؛

(دو) $\theta : \mathrm{Aut}_M N \cong \mathrm{Aut}_K E$.

در هر حالت، $\mathrm{Aut}_M N$ حلپذیر است (قضیهٔ II ۱۱۰۷۰) و N یک توسیع گالوای با بعد متناهی از K، و درنتیجه از M، می‌باشد. در حالت (یک) داریم

$$[N : M] = |\mathrm{Aut}_M N| < |\mathrm{Aut}_K E| = [E : K] = n$$

که از آنجا فرض استقرا ایجاب می‌کند که یک توسیع رادیکالی از M وجود دارد که شامل N است. همانطور که در اولین بند ذکر شد، این قضیه را در حالت (یک) ثابت می‌کند.

در حالت (دو)، فرض کنیم $J = \theta^{-1}(H)$. چون H در $\mathrm{Aut}_K E$ نرمال با اندیس J است، P در $\mathrm{Aut}_M N$ نرمال با اندیس J می‌باشد. به علاوه، طبق قضیهٔ II ۱۱۰۷۰، p حلپذیر است. هرگاه P میدان ثابت J (نسبت به $\mathrm{Aut}_M N$) باشد، آنگاه داریم

$$\begin{array}{ccc} N & \longleftrightarrow & 1 \\ \cup & & \triangle \\ P & \longleftrightarrow & J = \mathrm{Aut}_P N \\ \cup & & \triangle \\ M & \longleftrightarrow & \mathrm{Aut}_M N \end{array}$$

قضیهٔ اساسی ۵۰۲ ایجاب می‌کند که P روی M گالوا بوده و $\mathrm{Aut}_M P \cong \mathrm{Aut}_M N / J$. اما، طبق ساخت، $[\mathrm{Aut}_M N : J] = p$، که‌ازآنجا $\mathrm{Aut}_M P \cong Z_p$. بنابراین، P یک توسیع دوری از M بوده و $P = M(u)$، که در آن u ریشه‌ای از $x^p - a \in M[x]$ (تحویل‌ناپذیر) است (قضیهٔ ۱۱۰۷). لذا، P یک‌توسیع‌رادیکالی M بوده‌و $[N : P] < [N : M] = [F : K] = n$. چون $\mathrm{Aut}_P N = J$ حلپذیر بوده و N روی P گالواست (قضیهٔ ۵۰۲)، فرض استقرا ایجاب

می‌کند که یک توسیع رادیکالی مانند F از P وجود دارد که شامل N است. F بوضوح یک توسیع رادیکالی M است (تمرین ۴). این برهان را در حالت (دو) به پایان می‌برد.

نتیجهٔ ۷.۹. *فرض کنیم* K *یک میدان بوده و* $f \in K[x]$ *یک چندجمله‌ای از درجهٔ* $n > 0$ *باشد، که در آن* $char\ K$ ، $n!$ *را عاد نمی‌کند (که همواره وقتی* $char\ K = 0$ *درست است). در این صورت، معادلهٔ* $f(x) = 0$ *حلپذیر به وسیلهٔ رادیکالهاست اگر و فقط اگر گروه گالوای* f *حلپذیر باشد.*

طرح برهان. ($\Leftarrow$) فرض کنیم E یک میدان تجزیه‌گر f روی K باشد. در پرتو حکم ۶.۹، کافی است نشان دهیم که E روی K گالواست و $K \nmid [E:K]!$. چون داریم $K \nmid n!$، بنابر قضیهٔ III ۱۰.۶۰ و تمرین III ۳.۶۰، عوامل تحویل‌ناپذیر f جدایی‌پذیرند، که از آنجا E روی K گالواست (قضیهٔ ۱۱.۳ و تمرین ۱۳.۳). چون هر عدد اولی که $[E:K]!$ را عاد کند لزوماً $n!$ را عاد می‌کند (قضیهٔ ۲.۳)، نتیجه می‌گیریم که $K \nmid [E:K]$.

ضمیمه: معادلهٔ کلی از درجهٔ n

انگیزهٔ بحث ما با امتحان معادلات چندجمله‌ای از درجهٔ 2 روی میدان K با $char\ K \neq 2$ به بهترین وجه قابل مشاهده است. در اینجا و ذیلاً تحدید به چندجمله‌ایهای تکین صدمه‌ای به کلیت نمی‌زند. هرگاه t_1 و t_2 مجهولات باشند، آنگاه معادلهٔ

$$x^2 - t_1 x + t_2 = 0$$

روی میدان $K(t_1,t_2)$ از توابع گویا نسبت به t_1,t_2 ***معادله درجهٔ دوم کلی*** روی K نام دارد. یک معادلهٔ درجهٔ دوم (تکین) روی K را می‌توان، با گذاردن عناصر مناسبی از K به جای t_1 و t_2، از معادلهٔ درجهٔ دوم کلی به دست آورد. به آسانی تحقیق می‌شود که جوابهای معادلهٔ درجهٔ دوم کلی (در یک بست جبری از $K(t_1,t_2)$) عبارتند از

$$x = \frac{t_1 \pm \sqrt{t_1^2 - 4t_2}}{2},$$

که در آن به‌ازای $n \in \mathbf{Z}$، $n = n1_K$. این فرمول معروف درجهٔ دوم است. این فرمول نشان می‌دهد که جوابهای معادلهٔ درجهٔ دوم کلی در توسیع میدان رادیکالی $K(t_1,t_2)(u)$

که $u^2 = t_1^2 - 4t_2$ جا دارند. بـرای یافتن جوابهای $x^2 - bx + c = 0$ $(b,c \in K)$ ، کافی است b,c را به جای t_1,t_2 بگذاریم. واضح است که جوابها در توسیع رادیکالی $K(u)$ که $u^2 = b^2 - 4c \in K$ قراردارند. حال این ایده‌ها را به معادلات چندجمله‌ای از درجهٔ دلخواه تعمیم می‌دهیم.

فرض کنیم K یک میدان و n عددصحیح مثبتی باشد. میدان $K(t_1, \ldots, t_n)$ از توابع گویا روی K از مجهولات $t_1, \ldots, t_n$ را درنظر می‌گیریم. چندجمله‌ای

$$p_n(x) = x^n - t_1x^{n-1} + t_2x^{n-2} + \cdots + (-1)^{n-1}t_{n-1}x + (-1)^n t_n \in K(t_1, \ldots, t_n)[x]$$

چندجمله‌ای کلی از درجهٔ n روی K ، ومعادلهٔ $p_n(x) = 0$ **معادلهٔ کلی از درجهٔ n** روی K نام دارد[1]. توجه کنید که هر چندجمله‌ای (تکیی) از درجهٔ n در $K[x]$ ، مثلا $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ ، را می‌توان از چندجمله‌ای کلی $p_n(x)$ با گذاردن $(-1)^i a_i$ به جای t_i به دست آورد.

بحث پیشین تعریف زیر را طبیعی جلوه می‌دهد. گوییم یک **فرمول** برای جوابهای معادلهٔ کلی از درجهٔ n وجود دارد مشروط بر اینکه این معادله حلپذیر به وسیلهٔ رادیکالها روی میدان $K(t_1, \ldots, t_n)$ باشد. هرگاه $p_n(x) = 0$ حلپذیر به وسیلهٔ رادیکالها باشد، آنگاه جوابهای هر معادلهٔ چندجمله‌ای (تکیی) از درجهٔ n روی K را می‌توان با جانشانیهای مناسب درجوابهای $p_n(x) = 0$ به دست آورد. حال که این بدقت تنظیم شده است، می‌توان مسئلهٔ کلاسیکی که این بخش با آن شروع شد را سامان بخشید.

حکم ۸۰۹. (آبل[2]) *فرض کنیم K یک میدان و n عدد صحیح مثبتی باشد. معادلهٔ کلی از درجهٔ n حلپذیر به وسیلهٔ رادیکالهاست فقط اگر* $n \leq 4$.

چند تبصره. کلمات "فقط اگر" در حکم ۸۰۹ را می‌توان درصورتی‌که $\text{char } K = 0$ با "اگر و فقط اگر" عوض کرد. هرگاه توسیعهای رادیکالی همانند در تمرین ۲ تعریف شوند، آنگاه به‌ازای هر مشخص می‌توان "فقط اگر" را با "اگر و فقط اگر" عوض کرد. این امر که معادلهٔ کلی از درجهٔ n به‌ازای $n \geq 5$ حلپذیر به وسیلهٔ رادیکالها نیست امکان اینکه

---

۱. *علایم* $(-1)^i$ *برای ساده کردن محاسبات به کار رفته‌اند.*

2. Abel

یک معادلهٔ چندجمله‌ای خاص روی K از درجهٔ $n \geq 5$ حلپذیر به وسیلهٔ رادیکالهاست را مستثنی نمی‌کند.

طرح برهان ۸۰۹. فرض کنیم نمادگذاری مثل فوق بوده و $u_1, \ldots, u_n$ ریشه‌های $p_n(x)$ در میدان تجزیه‌گری مانند $F = K(t_1, \ldots, t_n)(u_1, \ldots, u_n)$ باشند. چون در F ، $p_n(x) = (x - u_1)(x - u_2)\cdots(x - u_n)$ ، محاسبه‌ای مستقیم نشان می‌دهد که

$$t_1 = \sum_{i=1}^{n} u_i;\ t_2 = \sum_{1 \leq i < j \leq n} u_i u_j;\ \ldots,\ t_n = u_1 u_2 \cdots u_n;$$

یعنی، $t_i = f_i(u_1, \ldots, u_n)$ ، که در آن $f_1, \ldots, f_n$ توابع متقارن مقدماتی از n مجهولند (ر.ک. ضمیمهٔ بخش ۲). پس نتیجه می‌شود که $F = K(u_1, \ldots, u_n)$. حال مجموعهٔ جدیدی از مجهولات $\{x_1, \ldots, x_n\}$ و میدان $K(x_1, \ldots, x_n)$ رادرنظر می‌گیریم. فرض کنیم E زیرمیدان تمام‌توابع گویای‌متقارن در $K(x_1, \ldots, x_n)$ باشد. ایدهٔ اصلی برهان ساختن یک یکریختی از میدانهای $K(x_1, \ldots, x_n)$ است به طوری‌که $F \cong K(t_1, \ldots, t_n)$ به روی E نگاشته شود. در این صورت، گروه گالوای $\mathrm{Aut}_{K(t_1,\ldots,t_n)}F$ از $p_n(x)$ با $\mathrm{Aut}_E K(x_1, \ldots, x_n)$ یکریخت است. اما $\mathrm{Aut}_E K(x_1, \ldots, x_n)$ با S_n یکریخت‌است (ر.ک.ص ۳۹۵). S_n حلپذیر است اگر و فقط اگر $n \leq 4$ (نتیجهٔ ۱۲۰۷۰ II و تمرین ۱۰۷۰ II). بنابراین، هرگاه $p_n(x) = 0$ حلپذیر به وسیلهٔ رادیکالها باشد، آنگاه، طبق نتیجهٔ ۵۰۹، $n \leq 4$! به عکس، هرگاه $n \leq 4$ و $\mathrm{char}\ K = 0$، آنگاه، طبق نتیجهٔ ۰۷۰۹ $p_n(x) = 0$ حلپذیر به وسیلهٔ رادیکالهاست.!

برای ساختن یکریختی $F \cong K(x_1, \ldots, x_n)$ ، ابتدا ملاحظه می‌کنیم که، طبق قضیهٔ ۱۸۰۲، زیرمیدان E از $K(x_1, \ldots, x_n)$ دقیقاً" مساوی $K(f_1, \ldots, f_n)$ است، که درآن $f_1, \ldots, f_n$ توابع متقارن مقدماتی‌اند. حال یک یکریختی حلقه‌ها مانند

$$K[t_1, \ldots, t_n] \cong K[f_1, \ldots, f_n]$$

را به صورت زیر می‌سازیم. بنابر قضیهٔ ۵۰۵۰ III، انتساب

$$g(t_1, \ldots, t_n) \mapsto g(f_1, \ldots, f_n)$$

(بخصوص، $t_i \mapsto f_i$) یک بروریختی حلقه‌ها مانند $\theta : K[t_1, \ldots, t_n] \to K[f_1, \ldots, f_n]$ را تعریف می‌کند. فرض‌کنیم $g(t_1, \ldots, t_n) \mapsto 0$؛ درنتیجه، در $K[f_1, \ldots, f_n] \subset K(x_1, \ldots, x_n)$ ، $g(f_1, \ldots, f_n) = 0$. طبق تعریف،

$$f_k = f_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

و درنتیجه ، $0 = g(f_1, \ldots, f_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. چون $g(f_1, \ldots, f_n)$ یک چندجمله‌ای از مجهولات $x_1, \ldots, x_n$ روی K بوده‌و $F = K(u_1, \ldots, u_n)$ میدانی شامل K می‌باشد ، با گذاردن u_i به جای x_i نتیجه می‌شود که

$$0 = g(f_1(u_1, \ldots, u_n), \ldots, f_n(u_1, \ldots, u_n)) = g(t_1, \ldots, t_n);$$

لذا ، θ یک تکریختی ، و درنتیجه یک‌یکریختی ، می‌باشد . به علاوه ، θ به یک یکریختی از میدانهای خارج‌قسمتی مانند $\theta : K(t_1, \ldots, t_n) \cong K(f_1, \ldots, f_n) = E$ توسیع می‌یابد (تمرین III ۷.۴۰) . اما $F = K(u_1, \ldots, u_n)$ یک‌میدان‌تجزیه‌گر $p_n(x)$ روی $K(t_1, \ldots, t_n)$ است و ، تحت نگاشت واضح القا شده به وسیلهٔ θ بر چندجمله‌ایها ،

$$p_n(x) \mapsto \bar{p}_n(x) = x^n - f_1 x^{n-1} + f_2 x^{n-2} - \cdots + (-1)^n f_n = (x - x_1)(x - x_2) \cdots (x - x_n)$$

(ر.ک. ص ۳۹۴) . واضح است که $K(x_1, \ldots, x_n)$ یک میدان تجزیه‌گر $\bar{p}_n(x)$ روی $K(f_1, \ldots, f_n) = E$ می‌باشد . بنابراین ، طبق قضیهٔ ۸.۳ ، یکریختی θ به یک یکریختی $K(t_1, \ldots, t_n)$ توسیع می‌یابدکه ، همانطورکه مطلوب است ، بنابر ساختن ، $F \cong K(x_1, \ldots, x_n)$ را به روی E می‌نگارد .

تمرینات

۱ . هرگاه F یک‌توسیع میدان‌رادیکالی از K و E یک میدان میانی باشد ، آنگاه F یک توسیع رادیکالی از E است .

۲ . فرض‌کنید "توسیع رادیکالی" به صورت زیر تعریف شده باشد : F توسیع رادیکالی K است اگر زنجیری متناهی‌از میدانها مانند $K = E_0 \subset E_1 \subset \cdots \subset E_n = F$ موجود باشد به‌طوری‌که ، به‌ازای هر $1 \le i \le n$ ، $E_i = E_{i-1}(u_i)$ و یکی از موارد زیر درست باشد : (یک) به‌ازای $m_i > 0$ ی ، $u_i^{m_i} \in E_{i-1}$ ؛ (دو) $\operatorname{char} K = p$ ونیز $u^p - u \in E_{i-1}$. مشابه‌های قضیهٔ ۴.۹ ، حکم ۶.۹ ، نتیجهٔ ۷.۹ ، و حکم ۸.۹ را بیان و اثبات کنید .

۳ . فرض‌کنید K یک میدان ، $f \in K[x]$ یک‌چندجمله‌ای‌تحویل‌ناپذیر از درجهٔ $n \ge 5$ ، و میدان F یک‌میدان‌تجزیه‌گر f روی K باشد . همچنین ، $\operatorname{Aut}_K F \cong S_n$. (ر.ک. مثال بعد از قضیهٔ ۱۲.۴) . فرض‌کنید u ریشه‌ای از f در F باشد . در این صورت ،

(آ) $K(u)$ روی K گالوا نیست؛ $[K(u):K]=n$ و $\mathrm{Aut}_K K(u)=1$ (و درنتیجه، حلپذیر است).

(ب) هر بست نرمال روی K که شامل u باشد شامل یک نسخهٔ یکریخت F است.

(پ) توسیع میدان رادیکالی مانند E از K باخاصیت $E \supset K(u) \supset K$ وجودندارد.

۴. هرگاه F یک توسیع میدان رادیکالی از E و E یک توسیع میدان رادیکالی از K باشد، آنگاه F یک توسیع رادیکالی از K می‌باشد.

۵. (کاردان[1]) فرض کنید K میدانی با $\mathrm{char}\, K \neq 2,3$ بوده و معادلهٔ مکعبی $x^3+a_1x^2+a_2x+a_3=0\ (a_i \in K)$ رادرنظر بگیریدو نیز فرض‌کنید $p=a_2-\frac{a_1^2}{3}$ و $q=\frac{2a_1^3}{27}-\frac{a_1a_2}{3}+a_3$. قرار دهید $P=\sqrt[3]{-q/2+\sqrt{p^3/27+q^2/4}}$ و $Q=\sqrt[3]{-q/2-\sqrt{p^3/27+q^2/4}}$ (که در آنها ریشه‌های مکعبی به طور مناسب اختیار شده‌اند). دراین صورت، جوابهای معادلهٔ داده شده عبارتند از $P+Q-a_1/3$، $\omega P+\omega^2 Q-a_1/3$، و $\omega^2 P+\omega Q-a_1/3$، که در آنها ω یک ریشهٔ مکعبی اولیهٔ واحد می‌باشد.

---

1. Cardan

۶

ساختار میدانها

در این فصل، توسیعهای میدان دلخواه یک میدان داده شده را تحلیل می‌کنیم. چون توسیعهای جبری به تفضیل در فصل پنج مطرح شدند، تاکید در اینجا بر توسیعهای متعالی خواهد بود. به عنوان اولین گام در این تحلیل، نشان خواهیم داد که هر توسیع میدان $K \subset F$ درواقع یک توسیع دومرحله‌ای $K \subset E \subset F$ است، که در آن F روی E جبری و E روی K صرفا" متعالی است (بخش ۱). مفهوم اصلی به کار رفته در اینجا یک پایهٔ تعالی است، که معلوم می‌شود که اصلیت آن (به نام درجهٔ تعالی) یک پایای توسیع K به وسیلهٔ F است (بخش ۱). در بخش ۲، مفهوم جدایی‌پذیری (احتمالا") به توسیعهای غیرجبری تعمیم یافته و چند توسیع جدایی‌پذیر به طرق مختلف توصیف خواهند شد.

۱ پایه‌های تعالی

قسمت اول این بخش به مفهوم استقلال جبری مربوط است، که تعمیم ایدهٔ استقلال خطی است. یک پایهٔ تعالی از میدان F روی زیرمیدان K مشابه (نسبت به استقلال جبری) با یک پایهٔ فضای برداری F روی K (نسبت به استقلال خطی) است. نشان می‌دهیم که اصلیت پایهٔ تعالی F روی K (درجهٔ تعالی) یک پایاست و خواص آن را مطالعه می‌کنیم. در این بخش از نماد u/v به جای uv^{-1}، که در آن u,v عناصری از یک میدانند و $v \neq 0$، مکرر استفاده خواهیم کرد. در سراسر این بخش K یک میدان می‌باشد.

تعریف ۱.۱ . فرض کنیم F یک توسیع میدان K بوده و S زیرمجموعه‌ای از F باشد.

S روی K **وابستهٔ جبری** است اگر به‌ازای عدد صحیح مثبتی چون n ، یک چندجمله‌ای ناصفر مانند $f \in K[x_1, \ldots, x_n]$ موجود باشدبه طوری‌که به‌ازای عناصر متمایزی مانند $s_1, \ldots, s_n \in S$ ، $f(s_1, \ldots, s_n) = 0$. S روی K **مستقل جبری** است اگر روی K وابستهٔ جبری نباشد .

چند تبصره . اغلب وقتی از قراین روشن باشد ، عبارت "روی K " را حذف می‌کنیم . زیرمجموعهٔ S از F روی K مستقل‌جبری‌است اگر به ازای هر $n > 0$ ، $f \in K[x_1, \ldots, x_n]$ ، و عناصر متمایز $s_1, \ldots, s_n \in S$ داشته باشیم

$$f(s_1, \ldots, s_n) = 0 \quad \Rightarrow \quad f = 0 .$$

هر زیرمجموعهٔ یک مجموعهٔ مستقل جبری مستقل جبری است . بخصوص ، مجموعهٔ پوچ مستقل جبری‌است . واضح است که هر زیرمجموعهٔ K وابستهٔ جبری است . مجموعهٔ $\{u\}$ روی K وابستهٔ‌جبری‌است اگر و فقط اگر u روی K جبری باشد . واضح است که هر عنصر یک مجموعهٔ مستقل جبری لزوما " روی K متعالی است . از اینرو ، اگر F روی K جبری باشد ، مجموعهٔ پوچ تنها زیرمجموعهٔ مستقل جبری F می‌باشد .

(وابستگی) استقلال جبری را می‌توان تعمیمی از مفهوم (وابستگی) استقلال خطی گرفت . زیرا مجموعهٔ S روی K وابستهٔ خطی است مشروط بر اینکه به‌ازای عدد صحیح مثبتی مانند n ، یک چندجمله‌ای‌ناصفر مانند f از **درجهٔ یک** در $K[x_1, \ldots, x_n]$ موجود باشدبه‌طوری‌که به‌ازای $s_i \in S$ های متمایزی ، $f(s_1, \ldots, s_n) = 0$. درنتیجه ، هر مجموعهٔ مستقل جبری مستقل خطی نیز هست ، ولی عکس آن درست **نیست** (ر.ک. مثال بعد از تعریف ۴۰۱ زیر) .

مثال . فرض کنیم K یک میدان‌باشد .در میدان توابع گویای $K(x_1, \ldots, x_n)$ ، مجموعهٔ مجهولات $\{x_1, \ldots, x_n\}$ روی K مستقل جبری است . به‌طور کلی ، داریم

قضیهٔ ۲۰۱ . فرض کنیم F یک توسیع میدان K بوده و $\{s_1, \ldots, s_n\}$ زیرمجموعه‌ای از F باشد که روی K مستقل جبری است . در این صورت ، K ــ یکریختی

$$K(s_1, \ldots, s_n) \cong K(x_1, \ldots, x_n)$$

وجود خواهد داشت.

طرح برهان. بنابرقضایای III ۵۰۵۰ و V ۳۰۱۰، انتساب $x_i \mapsto s_i$ یک K ــ بروریختی حلقه‌ها مانند $\theta : K[x_1, \ldots, x_n] \to K[s_1, \ldots, s_n]$ را تعریف می‌کند. استقلال جبری $\{s_1, \ldots, s_n\}$ ایجاب می‌کند که θ تکریختی باشد. بنابر نتیجهٔ III ۶۰۴۰، θ به یک K ــ تکریختی میدانهای $K(x_1, \ldots, x_n) \to K(s_1, \ldots, s_n)$ (که‌آن‌نیزبا θ نموده‌می‌شود) توسیع می‌یابدبه طوری‌که

$$\theta(f/g) = f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n) = f(s_1, \ldots, s_n)g(s_1, \ldots, s_n)^{-1}.$$

بنابر قضیهٔ V ۳۰۱۰ (پنج)، θ یک بروریختی‌است.

نتیجهٔ ۳۰۱۰. *به‌ازای $i = 1,2$ ، F_i را یک توسیع میدان K_i گرفته و فرض می‌کنیم $S_i \subset F_i$ ، که در آن S_i روی K_i مستقل جبری است. هرگاه $\varphi : S_1 \to S_2$ یک نگاشت انژکتیو از مجموعه‌ها بوده و $\sigma : K_1 \to K_2$ یک تکریختی میدانها باشد، آنگاه σ به یک تکریختی میدانهای $\bar{\sigma} : K_1(S_1) \to K_2(S_2)$ توسیع می‌یابد به‌طوری‌که، به‌ازای هر $s \in S_1$ ، $\bar{\sigma}(s) = \varphi(s)$. به‌علاوه، هرگاه φ بیژکتیوو σ یکریختی باشد، آنگاه $\bar{\sigma}$ یکریختی‌می‌باشد.*

تبصره. بخصوص، این نتیجه ایجاب می‌کند که هر جایگشت مجموعهٔ مستقل جبری S روی میدان K به یک K ــ خودریختی از $K(S)$ توسیع می‌یابد (کافی است قرار دهیم $K_1 = K = K_2$ و $\sigma = 1_K$).

طرح برهان ۳۰۱۰. به‌ازای هر $n \geq 1$ ، σ یک تکریختی حلقه‌ها مانند

$$K_1[x_1, \ldots, x_n] \to K_2[x_1, \ldots, x_n]$$

(که آن نیزبا σ نموده‌می‌شود؛ ر.ک. ص ۳۶۸) راالقا می‌کند. بنابر قضیهٔ V ۳۰۱۰، هر عنصر $K_1(S_1)$ به شکل $f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n)$ $(s_i \in S_1)$ است. برای راحتی، به‌جای $\varphi(s)$ می‌نویسیم φs و $\bar{\sigma} : K_1(S_1) \to K_2(S_2)$ را به‌صورت زیر تعریف می‌کنیم:

$$f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n) \mapsto \sigma f(\varphi s_1, \ldots, \varphi s_n)/\sigma g(\varphi s_1, \ldots, \varphi s_n) \in K(S_2).$$

به‌ازای هر زیرمجموعهٔ متناهی $\{s_1, \ldots, s_r\}$ از S_1 ، تحدید $\bar{\sigma}$ به $K_1(s_1, \ldots, s_r)$ ترکیب زیر است:

$$K_1(s_1, \ldots, s_r) \xrightarrow{\theta_1^{-1}} K_1(x_1, \ldots, x_r) \xrightarrow{\hat{\sigma}} K_2(x_1, \ldots, x_r) \xrightarrow{\theta_2} K_2(\varphi s_1, \ldots, \varphi s_r),$$

که درآن θ_i ها K_i ــ یکریختیهای قضیهٔ ۲۰۱ بوده و $\hat{\sigma}$ تکریختی منحصر به فرد میدانهای خارج قسمتی است که به وسیلهٔ $\sigma: K_1[x_1, \ldots, x_r] \to K_2[x_1, \ldots, x_r]$ القا شده و با $\hat{\sigma}(f/g) = (\sigma f)/(\sigma g)$ داده می‌شود (نتیجهٔ III ۶.۴۰). پس نتیجه می‌شود که $\bar{\sigma}$ یک تکریختی تعریف شده‌ای از میدانهاست. بنابر ساخت، σ به $\bar{\sigma}$ توسیع یافته و با φ بر S_1 یکی است. هرگاه σ یک یکریختی باشد، آنگاه هر $\hat{\sigma}$ نیز چنین است، که از آنجا $\theta_2\hat{\sigma}\theta_1^{-1}$ یک یکریختی می‌باشد. هرگاه φ بیژکتیو نیز باشد، $\bar{\sigma}$ یکریختی خواهد بود.

تعریف ۴۰۱. فرض کنیم F یک توسیع میدان K باشد. یک **پایهٔ تعالی** (یاپایهٔ) F روی K زیرمجموعه‌ای مانند S از F است که روی K مستقل جبری بوده و در مجموعهٔ تمام زیرمجموعه‌های مستقل جبری F (نسبت به شمول نظریهٔ مجموعه‌ها) ماکزیمال باشد.

وجود همیشگی پایه‌های تعالی فورا" از استدلالی با لم‌زرن نتیجه می‌شود (تمرین ۲). هرگاه تشابه بین استقلال جبری و خطی را به یاد آوریم، آنگاه یک پایهٔ تعالی مشابه یک پایهٔ فضای برداری است (زیرا، بنابر لم IV ۳.۲۰، یک چنین پایه دقیقا" یک زیرمجموعهٔ مستقل خطی ماکزیمال است). با اینحال، توجه کنید که یک پایهٔ تعالی یک پایهٔ فضای برداری نیست، اگرچه به عنوان یک مجموعهٔ مستقل خطی مشمول یک پایه می‌باشد (قضیهٔ IV ۴.۲۰).

مثال. هرگاه $f/g = f(x)/g(x) \in K(x)$ که $f, g \neq 0$، آنگاه چندجمله‌ای ناصفر $h(y_1, y_2) = g(y_1)y_2 - f(y_1) \in K[y_1, y_2]$ چنان است که $h(x, f/g) = g(x)[f(x)/g(x)] - f(x) = 0$. لذا، $\{x, f/g\}$ در $K(x)$ وابستهٔ جبری است. این استدلال نشان می‌دهد که $\{x\}$ یک پایهٔ تعالی $K(x)$ روی K است. مجموعهٔ $\{x\}$ یک پایه نیست، زیرا $\{1_K, x, x^2, x^3, \ldots\}$ در $K(x)$ مستقل خطی می‌باشد.

برای به‌دست آوردن توصیف مفیدی از پایه‌های تعالی، به قضیهٔ زیر نیاز خواهیم داشت.

قضیهٔ ۵.۱. فرض کنیم F یک توسیع میدان K بوده، زیرمجموعهٔ S از F روی K مستقل جبری باشد، و $u \in F - K(S)$. در این صورت، $S \cup \{u\}$ روی K مستقل جبری است اگر و فقط اگر u روی $K(S)$ متعالی باشد.

برهان. ($\Rightarrow$) هرگاه عناصر متمایزی چون $s_1, \ldots, s_{n-1} \in S$ و $f \in K[x_1, \ldots, x_n]$ ی موجود باشند به طوری‌که $f(s_1, \ldots, s_{n-1}, u) = 0$، آنگاه u ریشه‌ای از $f(s_1, \ldots, s_{n-1}, x_n) \in K(S)[x_n]$ است. اما $f \in K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$، که از آنجا

$$f = h_r x_n^r + h_{r-1} x_n^{r-1} + \cdots + h_1 x_n + h_0$$

که در آن هر $h_i \in K[x_1, \ldots, x_{n-1}]$. چون u روی $K(S)$ متعالی است، داریم $f(s_1, \ldots, s_{n-1}, x_n) = 0$. درنتیجه، به‌ازای هر i، $h_i(s_1, \ldots, s_{n-1}) = 0$. استقلال‌جبری S ایجاب می‌کند که، به‌ازای هر i، $h_i = 0$، که‌ازآنجا $f = 0$. بنابراین، $S \cup \{u\}$ مستقل جبری می‌باشد. ($\Leftarrow$) فرض کنیم $f(u) = 0$، که در آن $f = \sum_{i=0}^{n} a_i x^i \in K(S)[x]$.

بنابر قضیهٔ ۳.۱.۷، زیرمجموعه‌ای متناهی مانند $\{s_1, \ldots, s_r\}$ از S هست به طوری که، به‌ازای هر i، $a_i \in K(s_1, \ldots, s_r)$، که از آنجا، به‌ازای $f_i, g_i \in K[x_1, \ldots, x_r]$ ی،

$$a_i = f_i(s_1, \ldots, s_r)/g_i(s_1, \ldots, s_r).$$

فرض کنیم $g = g_1 g_2 \cdots g_n \in K[x_1, \ldots, x_r]$ و، به‌ازای هر i،

$$\bar{f}_i = f_i g_1 \cdots g_{i-1} g_{i+1} \cdots g_n \in K[x_1, \ldots, x_r].$$

در این صورت، $a_i = \bar{f}_i(s_1, \ldots, s_r)/g(s_1, \ldots, s_r)$ و

$$\begin{aligned} f(x) &= \sum a_i x^i = \sum \bar{f}_i(s_1, \ldots, s_r)/g(s_1, \ldots, s_r) x^i \\ &= g(s_1, \ldots, s_r)^{-1} (\sum \bar{f}_i(s_1, \ldots, s_r) x^i). \end{aligned}$$

(ما فقط "مخرج مشترکی" از ضرایب f را خارج کرده‌ایم.) فرض کنیم

$$h(x_1, \ldots, x_r, x) = \sum \bar{f}_i(x_1, \ldots, x_r) x^i \in K[x_1, \ldots, x_r, x].$$

چون $f(u) = 0$ و $g(s_1, \ldots, s_r)^{-1} \neq 0$، بایدداشته باشیم $h(s_1, \ldots, s_r, u) = 0$. استقلال جبری $S \cup \{u\}$ ایجاب می‌کند که $h = 0$، که از آنجا، به‌ازای هر i، $\bar{f}_i = 0$. لذا، هر $a_i = 0$ و $f = 0$. بنابراین، u روی $K(S)$ متعالی می‌باشد.

نتیجهٔ ۶.۱. فرض کنیم F یک توسیع میدان K بوده و زیرمجموعهٔ S از F روی K

مستقل جبری باشد. در این صورت، S یک پایهٔ تعالی F روی K است اگر و فقط اگر F روی K(S) جبری باشد.

برهان. تمرین.

چند تبصره. میدان F یک توسیع صرفاً "متعالی" میدان K است اگر $F = K(S)$، که در آن $S \subset F$ و S روی K مستقل‌جبری‌است. دراین حالت، بنابرنتیجهٔ ۶.۱، S لزوماً یک پایهٔ تعالی F روی K است. اگر F یک توسیع میدان دلخواه K باشد، S را یک پایهٔ تعالی F روی K گرفته و فرض می‌کنیم $E = K(S)$. نتیجهٔ ۶.۱ نشان می‌دهد که F روی E جبری است و E روی K صرفاً "متعالی" می‌باشد. بالاخره، نتیجهٔ ۶.۱ و تبصره‌های بعد از تعریف ۱.۱ نشان می‌دهند که F یک توسیع جبری K است اگر و فقط اگر مجموعهٔ پوچ یک پایهٔ تعالی F روی K باشد. در این حالت، مجموعهٔ پوچ بوضوح پایهٔ تعالی منحصر به فرد F روی K می‌باشد.

نتیجهٔ ۷.۱. هرگاه F یک توسیع میدان K بوده و، به‌ازای زیرمجموعه‌ای از F مانند X، F روی K(X) جبری باشد (بخصوص، هرگاه $F = K(X)$)، آنگاه X شامل یک پایهٔ تعالی از F روی K می‌باشد.

برهان. فرض کنیم S یک زیرمجموعهٔ مستقل جبری ماکزیمال X باشد (S بنابر استدلالی با لم‌زرن‌وجود دارد). در این صورت، طبق قضیهٔ ۵.۱، هر $u \in X - S$ روی $K(S)$ جبری‌است، که‌ازآنجا، طبق قضیهٔ ۱۲.۱.۷، $K(X)$ روی $K(S)$ جبری‌می‌باشد. درنتیجه، بنابر قضیهٔ ۱۳.۱.۷، F روی $K(S)$ جبری است. بنابراین، طبق نتیجهٔ ۶.۱، S یک پایهٔ تعالی F روی K است.

از تشابه با استقلال خطی و پایه‌ها انتظار می‌رود که هر دو پایهٔ تعالی یک اصلیت داشته باشند. همانند فضاهای برداری، برهان را به دو بخش تقسیم می‌کنیم.

قضیهٔ ۸.۱. فرض کنیم F یک‌توسیع میدان K باشد. هرگاه S یک پایهٔ تعالی متناهی

از F روی K باشد، آنگاه هر پایهٔ تعالی F روی K به اندازهٔ S عنصر دارد.

طرح برهان. فرض کنیم $S = \{s_1, \ldots, s_n\}$ و T یک پایهٔ تعالی باشد. حکم می‌کنیم که $t_1 \in T$ ی روی $K(s_2, \ldots, s_n)$ متعالی است. در غیر این صورت، هر عنصر T روی $K(s_2, \ldots, s_n)$ جبری است، که از آنجا، طبق قضیهٔ ۱۲۰۱۰ V، $K(s_2, \ldots, s_n)(T)$ روی $K(s_2, \ldots, s_n)$ جبری می‌باشد. چون F طبق نتیجهٔ ۶۰۱ روی $K(T)$ جبری است، F لزوماً روی $K(T)(s_2, \ldots, s_n) = K(s_2, \ldots, s_n)(T)$ جبری می‌باشد. بنابراین، طبق قضیهٔ ۱۳۰۱۰ V، F روی $K(s_2, \ldots, s_n)$ جبری می‌باشد. بخصوص، s_1 روی $K(s_2, \ldots, s_n)$ جبری است، که تناقض می‌باشد (قضیهٔ ۵۰۱). از اینرو، $t_1 \in T$ ی روی $K(s_2, \ldots, s_n)$ متعالی می‌باشد. درنتیجه، بنابر قضیهٔ ۵۰۱، $\{t_1, s_2, \ldots, s_n\}$ مستقل جبری خواهد بود.

اما، هرگاه s_1 روی $\{t_1, s_1, s_2, \ldots, s_n\}$ متعالی می‌بود، آنگاه $K(t_1, s_2, \ldots, s_n)$ بنابر قضیهٔ ۵۰۱ مستقل جبری می‌شد. این بوضوح غیرممکن است، زیرا S یک پایهٔ تعالی می‌باشد. بنابراین، s_1 روی $K(t_1, s_2, \ldots, s_n)$ جبری می‌باشد. درنتیجه، $K(S)(t_1) = K(t_1, s_2, \ldots, s_n)(s_1)$ روی $K(t_1, s_2, \ldots, s_n)$ جبری می‌باشد (قضیهٔ ۱۲۰۱۰ V)، که از آنجا F روی $K(t_1, s_2, \ldots, s_n)$ جبری می‌شود (قضیهٔ ۱۳۰۱۰ V و نتیجهٔ ۶۰۱). بنابراین، طبق نتیجهٔ ۶۰۱، $\{t_1, s_2, \ldots, s_n\}$ یک پایهٔ تعالی F روی K می‌باشد.

استدلالی مشابه نشان می‌دهد که $t_2 \in T$ ای روی $K(t_1, s_3, \ldots, s_n)$ متعالی است، که از آنجا $\{t_2, t_1, s_3, \ldots, s_n\}$ یک پایهٔ تعالی می‌باشد. اگر به استقرا عمل کنیم (در هر مرحله t_i را وارد و s_i را حذف نماییم)، مآلاً $t_1, t_2, \ldots, t_n \in T$ ای به دست می‌آوریم که $\{t_1, \ldots, t_n\}$ یک پایهٔ تعالی F روی K است. واضح است که باید داشته باشیم $T = \{t_1, \ldots, t_n\}$؛ و درنتیجه، $|S| = |T|$.

قضیهٔ ۹۰۱. *فرض کنیم F یک توسیع میدان K باشد. هرگاه S یک پایهٔ تعالی نامتناهی F روی K باشد، آنگاه هر پایهٔ تعالی F روی K اصلیتی مساوی S دارد.*

برهان. هرگاه T پایهٔ تعالی دیگری باشد، آنگاه، بنابر قضیهٔ ۸۰۱، T نامتناهی است. هرگاه $s \in S$، آنگاه، بنابر نتیجهٔ ۶۰۱، s روی $K(T)$ جبری است. ضرایب چندجمله‌ای تحویل‌ناپذیر f از s روی $K(T)$ همه در $K(T_s)$ قرار دارند که در آن T_s

زیرمجموعه‌ای متناهی از T است (قضیهٔ ۳۰۱۰۷) . درنتیجه ، $f \in K(T_s)[x]$ و s روی $K(T_s)$ جبری‌است . به‌ازای هر $s \in S$ ، زیرمجموعهٔ متناهی T_s از T را اختیار می‌کنیم .

نشان می‌دهیم‌که $\bigcup_{s\in S} T_s$ یک پایهٔ تعالی F روی K است . چون $\bigcup_s T_s \subset T$ ، این ایجاب می‌کند که $\bigcup_s T_s = T$. مجموعهٔ $\bigcup_s T_s$ ، به‌عنوان زیرمجموعه‌ای از T ، مستقل جبری است . به علاوه ، هر عنصر S روی $K(\bigcup_s T_s)$ جبری است . درنتیجه ، بنابر قضیهٔ ۱۲۰۱۰ ۷ ، $K(\bigcup_s T_s)(S)$ روی $K(\bigcup_s T_s)$ جبری است . چون $K(S) \subset K(\bigcup_s T_s)(S)$ ، هر عنصر $K(S)$ روی $K(\bigcup_s T_s)$ جبری‌است . چون F بنابرنتیجهٔ ۶۰۱روی $K(S)$ جبری است ، F روی $K(\bigcup_s T_s)$ نیزجبری‌است (ر.ک. قضیهٔ ۱۳۰۱۰ ۷) . بنابراین ، باز طبق نتیجهٔ ۶.۱ . $\bigcup_s T_s$ یک پایهٔ تعالی است ، که از آنجا $\bigcup_s T_s = T$.

بالاخره ، نشان می‌دهیم که $|T| \leq |S|$. لازم نیست مجموعه‌های T_s دو به دو ازهم جداباشندو این رامی‌توان‌به صورت زیر علاج کرد . مجموعهٔ S را مرتب می‌کنیم (آشنایی، بخش ۷) و عنصراول آن رابا 1 نشان‌می‌دهیم . فرض‌کنیم $T_1' = T_1$ و به‌ازای هر $1 < s \in S$ تعریف می‌کنیم $T_s' = T_s - \bigcup_{t<s} T_t$. واضح است که هر T_s' متناهی است . تحقیق کنیدکه $\bigcup_s T_s = \bigcup_s T_s'$ و T_s' ها دو به‌دوازهم جدایند . به‌ازای هر $s \in S$ ، ترتیب ثابتی برای عناصر T_s' اختیار می‌کنیم : $t_1, t_2, \ldots, t_{k_s}$. انتساب $t_i \mapsto (s,i)$ یک نگاشت انژکتیو مانند $\bigcup_s T_s' \to S \times \mathbf{N}^*$ تعریف می‌کند . بنابراین ، طبق تعریف ۳۰۸ و ۴۰۸ و قضیهٔ ۱۱۰۸ در آشنایی ، داریم

$$|T| = |\bigcup_s T_s| = |\bigcup_s T_s'| \leq |S \times \mathbf{N}^*| = |S||\mathbf{N}^*| = |S|\aleph_0 = |S|.$$

اگر در استدلال فوق نقش S و T باهم عوض شوند ، معلوم می‌شود که $|T| \leq |S|$ ، که از آنجا ، طبق قضیهٔ شرودر ــ برنشتاین ۶۰۸ در آشنایی ، $|S| = |T|$.

تعریف ۱۰۰۱ . فرض‌کنیم F یک توسیع میدان K باشد . **درجهٔ تعالی** F روی K (که با $tr.d.F/K$ نموده می‌شود) عدد اصلی $|S|$ است ، که در آن S یک پایهٔ تعالی F روی

K می‌باشد.

دو قضیهٔ فوق نشان می‌دهند که $\text{tr.d.}F/K$ از انتخاب S مستقل است. در تشابه بین استقلال جبری و خطی، $\text{tr.d.}F/K$ مشابه بعد فضای برداری $[F:K]$ است. تبصره‌ها و مثالهای بعد از تعریف ۴۰۱ نشان می‌دهند که $\text{tr.d.}F/K \leq [F:K]$ و $\text{tr.d.}F/K = 0$ اگر و فقط اگر F روی K جبری باشد.

قضیهٔ ۱۱۰۱. هرگاه F یک توسیع میدان E و E یک توسیع میدان K باشد، آنگاه

$$tr.d.\text{F/K} = (tr.d.\text{F/E}) + (tr.d.\text{E/K}).$$

برهان. فرض کنیم S یک پایهٔ تعالی E روی K و T یک پایهٔ تعالی F روی E باشد. چون $S \subset E$، S روی E وابستهٔ جبری است، که از آنجا $S \cap T = \varnothing$. کافی است نشان دهیم که $S \cup T$ یک پایهٔ تعالی F روی K است، زیرا در این صورت تعریف ۱۰۰۱ و تعریف ۳۰۸ در آشنایی ایجاب می‌کنند که

$$\text{tr.d.}F/K = |S \cup T| = |T| + |S| = (\text{tr.d.}F/E) + (\text{tr.d.}E/K).$$

پیش از هر چیز، هر عنصر E روی $K(S)$ (نتیجهٔ ۶۰۱)، و درنتیجه روی $K(S \cup T)$، جبری است. لذا، طبق قضیهٔ ۱۲۰۱۰ ۷، $K(S \cup T)(E)$ روی $K(S \cup T)$ جبری می‌باشد. چون

$$K(S \cup T) = K(S)(T) \subset E(T) \subset K(S \cup T)(E),$$

$E(T)$ روی $K(S \cup T)$ جبری می‌باشد. اما F روی $E(T)$ جبری است (نتیجهٔ ۶۰۱)؛ و لذا، طبق قضیهٔ ۱۳۰۱۰ ۷، روی $K(S \cup T)$ جبری می‌باشد. درنتیجه، بنابر نتیجهٔ ۶۰۱ کافی است نشان دهیم که $S \cup T$ روی K مستقل جبری است.

فرض کنیم f یک چندجمله‌ای روی K از $n+m$ متغیر باشد (که برای راحتی با $x_1, \ldots, x_n, y_1, \ldots, y_m$ نموده می‌شود) به‌طوری‌که، به‌ازای $s_1, \ldots, s_n \in S$، $t_1, \ldots, t_m \in T$ متمایزی، $f(s_1, \ldots, s_n, t_1, \ldots, t_m) = 0$. فرض کنیم

$$g = g(y_1, \ldots, y_m) = f(s_1, \ldots, s_n, y_1, \ldots, y_m) \in K(S)[y_1, \ldots, y_m] \subset E[y_1, \ldots, y_m].$$

چون $g(t_1, \ldots, t_m) = 0$، استقلال جبری T روی E ایجاب می‌کند که $g = 0$. اما

$$f = f(x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{i=1}^{r} h_i(x_1, \ldots, x_n)k_i(y_1, \ldots, y_m)$$

، که در آن

$$h_i \in K[x_1, \ldots, x_n], k_i \in K[y_1, \ldots, y_m].$$

از اینرو $0 = g(y_1, \ldots, y_m) = f(s_1, \ldots, s_n, y_1, \ldots, y_m)$ ایجاب می‌کندکه، به‌ازای هر i ، $h_i(s_1, \ldots, s_n) = 0$. استقلال‌جبری S روی K ایجاب می‌کندکه، به‌ازای‌هر i ، $h_i = 0$ ، که از آنجا $f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$. بنابراین، $S \cup T$ روی K مستقل جبری می‌باشد.

هرگاه K_1 و K_2 میدانهایی با بستهای جبری F_1, F_2 باشند، آنگاه قضیهٔ ۸.۳۰ V ایجاب می‌کند که هر یکریختی $K_1 \cong K_2$ به یک یکریختی مانند $F_1 \cong F_2$ توسیع می‌یابد. تحت مفروضاتی مناسب می‌توان این نتیجه را به حالتی‌که در آن میدانهای F_i به‌طور جبری بسته‌اند ولی لزوما " روی K_i جبری نیستند تعمیم داد.

قضیهٔ ۱۲.۱ . فرض کنیم $F_1 \mid F_2$ یک توسیع میدان به‌طور جبری بستهٔ میدان $K_1 \mid K_2$ باشد. هرگاه $tr.d.F_1/K_1 = tr.d.F_2/K_2$ ، آنگاه هر یکریختی میدانهای $K_1 \cong K_2$ به یک یکریختی مانند $F_1 \cong F_2$ توسیع می‌یابد.

برهان. فرض کنیم S_i یک پایهٔ تعالی F_i روی K_i باشد. چون $|S_1| = |S_2|$ ، بنابر نتیجهٔ ۳.۱ ، $\sigma : K_1 \cong K_2$ به یک یکریختی مانند $\bar{\sigma} : K_1(S_1) \cong K_2(S_2)$ توسیع می‌یابد. F_i روی $K_i(S_i)$ به طور جبری بسته و جبری است (نتیجهٔ ۶.۱)؛ و درنتیجه، یک بست جبری $K_i(S_i)$ است. بنابراین، طبق قضایای ۴.۳۰ V و ۸.۳۰ V ، $\bar{\sigma}$ به یک یکریختی مانند $F_1 \cong F_2$ توسیع خواهد یافت.

تمرینات

تذکر. F همواره یک توسیع میدان‌از میدان K است.

۱. (خاصیت تعویض) فرض‌کنید S زیرمجموعه‌ای از F باشد. هرگاه $u \in F$ روی $K(S)$ جبری بوده و u روی $K(S - \{v\})$ ، که $v \in S$ ، جبری نباشد، آنگاه v روی $K((S - \{v\}) \cup \{u\})$ جبری نخواهد بود.

۲. (آ) با استفاده از لم‌زرن، نشان‌دهیدکه‌هرتوسیع میدان دارای یک پایهٔ تعالی است.

(ب) هر زیرمجموعهٔ مستقل جبری از F مشمول یک پایهٔ تعالی است.

۳ . $\{x_1, \ldots, x_n\}$ یک پایهٔ تعالی $K(x_1, \ldots, x_n)$ است .

۴ . هرگاه E_1, E_2 میدانهایی میانی باشند ، آنگاه

(یک) به‌ازای $i = 1,2$ ، $\text{tr.d.}E_1E_2/K \geq \text{tr.d.}E_i/K$ ؛

(دو) $\text{tr.d.}E_1E_2/K \leq (\text{tr.d.}E_1/K) + (\text{tr.d.}E_2/K)$.

۵ . هرگاه $F = K(u_1, \ldots, u_n)$ یک توسیع با تولید متناهی از K بوده و E یک میدان میانی باشد ، آنگاه E یک توسیع با تولید متناهی از K می‌باشد .

[**تذکر .** بنابر قضایای V ۱۱۰۱۰ و V ۱۲۰۱۰ ، حالت جبری بدیهی است .]

۶ . (آ) هرگاه S یک پایهٔ تعالی از میدان اعداد مختلط $\mathbf{C}$ روی میدان اعداد گویای $\mathbf{Q}$ باشد ، آنگاه S نامتناهی است . [**راهنمایی .** نشان دهید هرگاه S متناهی باشد ، آنگاه

$$|\mathbf{Q}(S)| = |\mathbf{Q}(x_1, \ldots, x_n)| = |\mathbf{Q}[x_1, \ldots, x_n]| = |\mathbf{Q}| < |\mathbf{C}|$$

(ر.ک. تمرینهای ۳۰۸ و ۹۰۸ آشنایی و قضیهٔ ۲۰۱) . اما لم V ۵۰۳۰ ایجاب می‌کند که $|\mathbf{Q}(S)| = |\mathbf{C}|$.]

(ب) بی‌نهایت خودریختی متمایز از میدان $\mathbf{C}$ وجود دارند .

(پ) $\text{tr.d.}\mathbf{C}/\mathbf{Q} = |\mathbf{C}|$.

۷ . هرگاه F به‌طورجبری‌بسته‌بوده و E میدانی‌میانی‌باشدبه‌طوری‌که $\text{tr.d.}E/K$ متناهی است، آنگاه هر K ــ تکریختی $E \to F$ به یک K ــ خودریختی F توسیع می‌یابد .

۸ . هرگاه F به‌طورجبری بسته‌بوده و $\text{tr.d.}F/K$ متناهی باشد ، آنگاه هر K ــ تکریختی $F \to F$ عملا " یک خودریختی است .

۲ ازهم جدایی خطی و جدایی‌پذیری

هدف اصلی این بخش تعمیم مفهوم جدایی‌پذیری به توسیعهای میدان (احتمالا ") غیرجبری است . این مفهوم کلیتر جدایی‌پذیری با تعریف قبلی ما در حالت توسیعهای جبری سازگاراست (قضیهٔ ۸۰۲) . ابتدا ایدهٔ ازهم جدایی خطی را معرفی کرده و خواص اساسی آن را عرضه می‌کنیم (قضایای ۲۰۲ تا ۷۰۲) . جدایی‌پذیری را برحسب ازهم جدایی خطی تعریف کرده و به طرق مختلف توصیف می‌کنیم (قضیهٔ ۱۰۰۲) . خواص دیگر جدایی‌پذیری در نتایج قضیهٔ ۱۰۰۲ آمده‌اند .

در بحث زیر تمام میدانها زیرمیدان میدان به‌طور جبری بستهٔ (ثابت) C گرفته

می‌شوند .

تعریف ۱۰۲ . فرض کنیم C یک میدان به‌طور جبری بسته و K,E,F زیرمیدانهای آن باشند به‌طوری‌که $K \subset E \cap F$. E و F روی K *ازهم جدای خطی‌اند* اگر هر زیرمجموعهٔ E که روی K مستقل خطی است روی F نیز مستقل خطی باشد .

چند تبصره . تعریفی دیگر برحسب حاصل‌ضربهای تانسوری در تمرین ۱ داده شده است . توجه کنید که زیرمجموعهٔ X از E روی یک زیرمیدان C مستقل خطی است اگر و فقط اگر هر زیرمجموعهٔ متناهی X چنین باشد . درنتیجه ، وقتی ازهم جدایی خطی را ثابت می‌کنیم ، فقط کافی است به مجموعه‌های مستقل خطی متناهی بپردازیم .

مثال . هرگاه $K \subset E$ ، آنگاه E و K بر K بداهتا " ازهم جدای خطی‌اند . این امر در چند برهان به کار خواهد رفت . مثالهایی کمتر بدیهی در قضایا و تمرینات زیر خواهند آمد .

از تعریف ۱۰۲ چنین برمی‌آید که تعریف ازهم جدایی خطی عملا " نسبت به E و F متقارن است . حال این مطلب را ثابت می‌کنیم .

قضیهٔ ۲۰۲ . *فرض کنیم C یک میدان به‌طور جبری بسته با زیرمیدانهای K,E,F باشد به‌طوری‌که* $K \subset E \cap F$. *در این صورت ، E و F روی K ازهم جدای خطی‌اند اگر و فقط اگر F و E روی K ازهم جدای خطی باشند .*

برهان . کافی است فرض کنیم E و F ازهم جدای خطی باشند و نشان دهیم که F و E ازهم جدای خطی‌اند . فرض کنیم $X \subset F$ روی K مستقل خطی باشد ولی روی E نباشد ؛ درنتیجه ، به‌ازای $u_i \in X$ هایی و $r_i \in E$ هایی‌که همه صفرنیستند ، $r_1u_1 + \cdots + r_nu_n = 0$. زیرمجموعهٔ $\{r_1, \ldots, r_n\}$ را اختیار می‌کنیم که نسبت به استقلال خطی روی K ماکزیمال است ؛ در صورت لزوم آن را اندیسگذاری مجدد می‌کنیم ؛ درنتیجه ، این مجموعه مساوی است با $\{r_1, r_2, \ldots, r_t\}$ $(t \geq 1)$. در این صورت ، به‌ازای هر $a_{ij} \in K$ ، $r_j = \sum_{i=1}^{t} a_{ij}r_i$ ، که

در آن $j > t$ (تمرین IV ۱۰۲۰). پس از تغییر بی‌ضرر اندیس، داریم

$$0 = \sum_{j=1}^{n} r_j u_j = \sum_{j=1}^{t} r_j u_j + \sum_{j=t+1}^{n} \left(\sum_{i=1}^{t} a_{ij} r_i \right) u_j$$
$$= \sum_{k=1}^{t} \left(u_k + \sum_{j=t+1}^{n} a_{kj} u_j \right) r_k.$$

چون E و F ازهم جدای خطی‌اند، $\{r_1, \ldots, r_t\}$ روی F مستقل خطی است، که ایجاب می‌کند که به‌ازای هر $k \leq t$، $u_k + \sum_{j=t+1}^{n} a_{kj} u_j = 0$. این با استقلال خطی X روی K متناقض است. بنابراین، X روی E مستقل خطی می‌باشد.

لم و قضیهٔ زیر محکهای مفیدی برای ازهم جدایی خطی دو میدان به دست می‌دهند.

لم ۳۰۲. *فرض کنیم C یک میدان به‌طور جبری بسته با زیرمیدانهای K,E,F باشد به طوری‌که $K \subset E \cap F$. همچنین، R زیرحلقه‌ای از E باشد به‌طوری‌که $K(R) = E$ و $K \subset R$ (که ایجاب می‌کند که R یک‌فضای‌برداری روی K باشد). در این صورت، شرایط زیر با هم معادلند:*

(یک) E و F روی K ازهم جدای خطی‌اند؛

(دو) هر زیرمجموعهٔ R که روی K مستقل خطی باشد روی F نیز مستقل خطی است؛

(سه) یک پایه از R روی K وجود دارد که روی F مستقل خطی است.

تبصره. لم با مفروضات ضعیفتر نیز برقرار است (تمرین ۲)، اما این تمام چیزی است‌که نیاز خواهیم داشت.

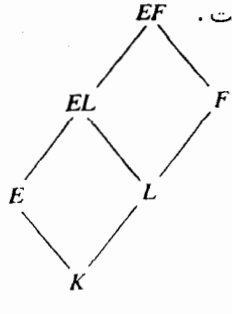
برهان ۳۰۲. (دو) $\Rightarrow$ (یک) و (سه) $\Rightarrow$ (یک) بدیهی‌اند. (یک) $\Rightarrow$ (دو) فرض کنیم $X = \{u_1, \ldots, u_n\}$ زیرمجموعه‌ای متناهی از E باشد که روی K مستقل خطی است. باید نشان دهیم که X روی F مستقل خطی است. چون $u_i \in E = K(R)$، هر u_i به شکل $u_i = c_i d_i^{-1} = c_i/d_i$ است، که در آن $c_i = f_i(r_1, \ldots, r_{t_i})$، $0 \neq d_i = g_i(r_1, \ldots, r_{t_i})$، به‌ازای $r_i \in R$ و $f_i, g_i \in K[x_1, \ldots, x_{t_i}]$ (قضیهٔ ۳۰۱۰ V). فرض کنیم $d = d_1 d_2 \cdots d_n$ و، به‌ازای

هر i ، $v_i = c_1 d_1 \cdots d_{i-1} d_{i+1} \cdots d_n \in R$. در این صورت ، $u_1 = v_1 d^{-1}$ و زیر مجموعهٔ $X' = \{v_1, \ldots, v_n\}$ از R روی زیرمیدانی از C مستقل خطی است اگر و فقط اگر X چنین باشد . طبق فرض، X ، و درنتیجه X' ، روی K مستقل خطی است . درنتیجه ، (دو) ایجاب می‌کند که X' روی F مستقل خطی باشد ، که از آنجا X روی F مستقل خطی می‌باشد .

(دو) ⇒ (سه) فرض کنیم U پایه‌ای از R روی K باشد که روی F مستقل خطی است . باید نشان دهیم که هر زیرمجموعهٔ متناهی X از R که روی K مستقل خطی باشد روی F نیز مستقل خطی است . چون X متناهی است ، زیرمجموعه‌ای متناهی مانند U_1 از U هست به طوری که X مشمول K ــ زیرفضای V از R است که به وسیلهٔ U_1 پیموده می‌شود (توجه کنید که U_1 یک پایهٔ V روی K است) . فرض کنیم V_1 فضای برداری پیموده شده به‌وسیلهٔ U_1 روی F باشد . بنابر (سه) U ، و درنتیجه U_1 ، روی F مستقل خطی است . بنابراین ، U_1 یک پایهٔ V_1 روی F بوده و $\dim_K V = \dim_F V_1$. اما X مشمول پایه‌ای متناهی مانند W از V روی K است (قضیهٔ IV ۴۰۲۰) . چون W ، به عنوان یک فضای برداری روی F ، مسلما " V_1 را می‌پیماید ، W شامل پایهٔ W_1 از V_1 روی F است . لذا ، $|W_1| \leq |W| = \dim_K V = \dim_F V_1 = |W_1|$ ، که از آنجا $W = W_1$. بنابراین ، زیرمجموعهٔ X از W لزوما " روی F مستقل خطی می‌باشد .

قضیهٔ ۴۰۲ . *فرض کنیم C یک میدان به‌طور جبری بسته با زیرمیدانهای K,E,L,F باشد به‌طوری که* $K \subset E$ و $K \subset L \subset F$. *دراین صورت ، E و F روی K ازهم جدای خطی‌اند اگر و فقط اگر (یک) E و L روی K ازهم جدای خطی بوده و (دو) EL و F روی L ازهم‌جدای خطی باشند .*

برهان . وضعیت به شکل زیر است .



($\Rightarrow$) هرگاه زیرمجموعهٔ X از E روی K مستقل خطی باشد، آنگاه، بنابر (یک)، X روی L مستقل خطی است. بنابراین (چون $X \subset E \subset EL$)، طبق قسمت (دو)، X روی F مستقل خطی می‌باشد.

($\Leftarrow$) هرگاه E و F روی K ازهم جدای خطی باشند، آنگاه E و L خود به خود روی K ازهم جدای خطی‌اند. برای اثبات (دو)، ملاحظه می‌کنیم که $EL = L(R)$، که در آن R زیرحلقهٔ $L[E]$ از C است که به‌وسیلهٔ L و E تولید می‌شود. بنابر قضیهٔ ۳۰۱۰ V، هر عنصر R به شکل $f(e_1, \ldots, e_n)$ $(e_i \in E; f \in L[x_1, \ldots, x_n])$ است. بنابراین، هر پایهٔ U از E روی K، R را به عنوان فضایی برداری روی L می‌پیماید. چون E و L روی K ازهم جدای خطی‌اند، U روی L مستقل خطی است. از اینرو، U یک پایهٔ R روی L است. اما، طبق ازهم‌جدایی‌خطی E و F، U روی F مستقل خطی است. بنابراین، طبق لم ۳۰۲، EL و F روی L ازهم جدای خطی‌اند.

حال ازهم جدایی خطی نسبت به توسیعهای میدان خاصی از K را بررسی می‌کنیم که در تعریف جدایی‌پذیری نقش مهمی دارند.

تعریف ۵۰۲. فرض کنیم K میدانی با مشخص $p \neq 0$ بوده و C یک میدان به‌طور جبری بسته و شامل K باشد. به‌ازای هر عدد صحیح $n \geq 0$،

$$K^{1/p^n} = \{u \in C \mid u^{p^n} \in K\}.$$
$$K^{1/p^\infty} = \bigcup_{n \geq 0} K^{1/p^n} = \{u \in C \mid u^{p^n} \in K \text{ ، ی } n \geq 0 \text{ به‌ازای }\}$$

چند تبصره. چون در یک میدان با مشخص p، $(u \pm v)^{p^n} = u^{p^n} \pm v^{p^n}$ (تمرین III ۱۱۰۱۰)، هر K^{1/p^n} عملاً یک میدان است. چون به‌ازای هر n,m که $0 \leq n \leq m$، $K = K^{1/p^0} \subset K^{1/p^n} \subset K^{1/p^m} \subset K^{1/p^\infty}$ نیز میدان است. به طور جبری بسته بودن C ایجاب می‌کند که K^{1/p^n} یک میدان تجزیه‌گر مجموعهٔ چندجمله‌ایهای $\{x^{p^n} - k \mid k \in K\}$ روی K باشد (تمرین ۵). بخصوص، هر $k \in K$ به‌ازای $v \in K^{1/p^n}$ ای به شکل v^{p^n} است. چون K^{1/p^n} یک میدان تجزیه‌گر روی K است، لزوماً مستقل از C می‌باشد (یعنی، بنابر قضیهٔ ۸۰۳۰ V، انتخاب دیگر C' یک نسخهٔ یکریخت K^{1/p^n} به‌دست می‌دهد).

لم ۶.۲ . *هرگاه F یک توسیع میدان K با مشخص $p \neq 0$ بوده و C یک میدان به‌طور جبری‌بستهٔ شامل F باشد ، آنگاه ، به‌ازای هر $n \geq 0$ ، زیرمجموعهٔ X از F روی K^{1/p^n} مستقل‌خطی‌است‌اگر و فقط‌اگر $X^{p^n} = \{u^{p^n} \mid u \in X\}$ روی K مستقل خطی باشد . به علاوه ، X روی K^{1/p^∞} مستقل خطی است اگر و فقط‌اگر ، به‌ازای هر $n \geq 0$ ، روی K^{1/p^n} مستقل خطی باشد .*

طرح برهان . هر $a \in K$ به‌ازای $v \in K^{1/p^n}$ ای به شکل $a = v^{p^n}$ است (تمرین ۵) . برای حکم اول توجه کنید که

$$\sum_i a_i u_i^{p^n} = 0 \ (a_i \in K;\ u_i \in X) \Leftrightarrow \sum_i v_i^{p^n} u_i^{p^n} = 0 \ (v_i \in K^{1/p^n}$$

$$v_i^{p^n} = a_i) \Leftrightarrow (\sum_i v_i u_i)^{p^n} = 0 \Leftrightarrow \sum_i v_i u_i = 0 .$$

برای حکم دوم ملاحظه کنید که هرگاه $(w_i \in K^{1/p^\infty};\ u_i \in X) \sum_{i=1}^{t} w_i u_i = 0$ ، آنگاه ، به‌ازای n به قدرکافی بزرگ ، $w_1, \ldots, w_t \in K^{1/p^n}$.

قضیهٔ ۷.۲ . *فرض‌کنیم میدان F مشمول میدانی به‌طور جبری بسته مانند C باشد . هرگاه F یک توسیع صرفا " متعالی از میدان K با مشخص $p \neq 0$ باشد ، آنگاه ، به‌ازای هر $n \geq 0$ ، F و K^{1/p^n} روی K ازهم‌جدای‌خطی‌اند و F و K^{1/p^∞} روی K ازهم جدای خطی می‌باشند .*

برهان . فرض‌کنیم $F = K(S)$ ، که در آن S یک پایهٔ تعالی F روی K باشد . هرگاه $S = \varnothing$ ، آنگاه $F = K$ و هر زیرمجموعهٔ مستقل خطی از F روی K دقیقا " از یک عنصر ناصفر K تشکیل شده است . واضح است که یک چنین مجموعهٔ یکانی ناصفر روی هر زیرمیدان C مستقل‌خطی‌است ،که‌از آنجا قضیه به‌ازای $S = \varnothing$ برقرار است . اگر S تهی نباشد ، M را مجموعهٔ‌تکجمله‌ایهاروی S می‌انگاریم . (یعنی ،مجموعهٔ‌تمام‌حاصل‌ضربهای متناهی‌عناصر S). دراین‌صورت ، M روی K مستقل خطی است ،زیرا S روی K مستقل جبری است . بنابر قضیهٔ ۳.۱۰ V ، M زیرحلقهٔ $K[S]$ را (به‌عنوان فضایی برداری روی K) می‌پیماید . بنابراین ، M روی K یک پایه‌از $K[S]$ است . استقلال‌جبری S ایجاب می‌کند که به‌ازای هر $n \geq 0$ ، $M^{p^n} = \{m^{p^n} \mid m \in M\}$ روی K مستقل‌خطی‌باشد . بنابرلم ۶.۲ ،

به‌ازای هر n ، M روی K^{1/p^n} ، و درنتیجه روی K^{1/p^∞} ، مستقل خطی است. بنابراین، طبق لم ۳۰۲ (به‌ازای $K[S], F, K^{1/p^n}$ به‌ترتیب به جای R, E, F) به‌ازای هر $0 \le n \le \infty$ ، F و K^{1/p^n} روی K ازهم جدای خطی‌اند.

قضیهٔ زیر رابطهٔ بین ازهم جدایی خطی وتوسیعهای جبری‌جدایی‌پذیر رانشان داده و تعریف جدایی‌پذیری در حالت توسیعهای دلخواه (احتمالا "غیرجبری") را موجب می‌شود.

قضیهٔ ۸۰۲. *فرض کنیم F یک‌توسیع میدان جبری از میدان K با مشخص $p \neq 0$ بوده و C یک میدان به‌طورجبری‌بسته‌و شامل F باشد. در این صورت، F روی K جدایی‌پذیر است اگر و فقط اگر F و $K^{1/p}$ روی K ازهم جدای خطی باشند.*

برهان. در اینجا فقط ثابت می‌کنیم جدایی‌پذیری ایجاب می‌کند که F و $K^{1/p}$ ازهم جدای‌خطی باشند. نیمهٔ دیگر برهان نتیجهٔ ساده‌ٔ مطلب زیر است (ر.ک. تبصره‌های بعد از قضیهٔ ۱۰۲). فرض کنیم $X = \{u_1, \dots, u_n\}$ زیرمجموعه‌ای متناهی از F باشدکه روی K مستقل خطی است. باید نشان دهیم‌که X روی $K^{1/p}$ مستقل‌خطی‌است. زیرمیدان $E = K(u_1, \dots, u_n)$ روی K با بعدمتناهی‌بوده (قضیهٔ ۱۲۰۱۰ V) و دارای پایه‌ای مانند $\{u_1, \dots, u_n, u_{n+1}, \dots, u_r\}$ شامل X است (قضیهٔ ۴۰۲۰ IV). هرگاه $v \in E$ و k عدد صحیح‌مثبتی‌باشد، آنگاه $v^k = \sum_{i=1}^{r} a_i u_i \quad (a_i \in K)$ ؛ودرنتیجه، $v^{kp} = (\sum_i a_i u_i)^p = \sum a_i^p u_i^p$.

چون v روی K جدایی‌پذیر است، $K(v)$ روی $K(v^p)$ هم جبری جدایی‌پذیر و هم صرفا" جدایی‌ناپذیر است (قضیهٔ ۴۰۶۰ V و لم ۶۰۶۰ V)؛ که از آنجا $K(v) = K(v^p) = K[v^p]$ (قضایای ۶۰۱۰ V و ۲۰۶۰ V). لذا، v ترکیبی خطی از v^{kp} ، و درنتیجه از u_i^p ، می‌باشد. بنابراین، E به وسیلهٔ $\{u_1^p, \dots, u_r^p\}$ پیموده می‌شود. چون $[E : K] = r$ ، $\{u_1^p, \dots, u_r^p\}$ بنابرقضایای ۵۰۲۰ IV و ۷۰۲۰ IV بایدپایه‌باشد. لذا، $\{u_1^p, \dots, u_r^p\}$ ، و درنتیجه X^p ، روی K مستقل‌خطی است. بنابر لم ۶۰۲ ، X روی $K^{1/p}$ مستقل خطی است، که از آنجا F و $K^{1/p}$ روی K ازهم جدای خطی می‌باشند.

تعریف ۹۰۲. فرض کنیم F یک توسیع میدان K باشد. هر پایهٔ تعالی S از F روی

K یک پایهٔ تعالی **جداگر** F روی K نام دارد اگر F روی $K(S)$ جبری جدایی‌پذیر باشد. هرگاه F دارای پایهٔ تعالی جداگر روی K باشد، آنگاه گوییم F روی K **به‌طور جدایی‌پذیر تولید شده است.**

چند تبصره. به‌یاد آورید که F روی $K(S)$ جبری است (نتیجهٔ ۶.۱). اگر F روی K به‌طور جدایی‌پذیر تولید شده باشد، درست نیست که هر پایهٔ تعالی F روی K لزوماً یک پایهٔ تعالی جداگر است (تمرین ۸).

چند مثال. هرگاه F روی K جبری جدایی‌پذیر باشد، آنگاه مجموعهٔ پوچ یک پایهٔ تعالی جداگر است. هرتوسیع صرفاً متعالی بداهتاً به‌طور جدایی‌پذیر تولید شده است، زیرا $F = K(S)$.

برای داشتن قضیهٔ مهمی که درحالت مشخص صفر با معنی باشد، (به‌ازای هر میدان K ی با مشخص 0) تعریف می‌کنیم $K^{1/0} = K^{1/0^n} = K^{1/0^\infty} = K$.

قضیهٔ ۱۰.۲. *هرگاه F یک توسیع میدان ازمیدان K بامشخص $p \geq 0$ بوده و C یک میدان به‌طور جبری بستهٔ شامل F باشد، آنگاه شرایط زیر باهم معادلند:*

(یک) F و $K^{1/p}$ روی K ازهم جدای جبری‌اند؛

(دو) به‌ازای $n \geq 1$ ی، F و K^{1/p^n} روی K ازهم جدای خطی‌اند؛

(سه) F و K^{1/p^∞} روی K ازهم جدای خطی‌اند؛

(چهار) هر میدان‌میانی باتولیدمتناهی E روی K به‌طور جدایی‌پذیر تولید شده است؛

(پنج) K_0 و F روی K ازهم جدای خطی‌اند، که در آن K_0 میدان ثابت (نسبت به C و K) $Aut_K C$ می‌باشد.

چند تبصره. قضیه ذیلاً ثابت می‌شود. استلزام (چهار) $\Rightarrow$ (یک) برهانی از نیمهٔ دوم قضیهٔ ۸.۲ بـه صورت زیر به دست می‌دهد. به‌ازای هر $u \in F$، $K(u)$ یک میدان میانی با تولید متناهی است؛ و لذا، روی K به‌طور جدایی‌پذیر تولید شده است. اما F (و درنتیجه، $K(u)$) روی K جبری فرض شده است و تنها پایهٔ تعالی یک توسیع جبری

مجموعهٔ پـوچ است. بنابراین، $K(u)$ روی میدان $K(\varnothing) = K$ جبری جدایی‌پذیر است. از اینرو، هر $u \in F$ روی K جبری جدایی‌پذیر می‌باشد.

طرح برهان ۱۰.۲. جز در برهان (چهار) $\Leftrightarrow$ (سه)، فرض می‌کنیم $\operatorname{char} K = p \neq 0$، زیراحالت $\operatorname{char} K = 0$ بدیهی‌است. (یک) $\Rightarrow$ (دو) $\Rightarrow$ (سه) بی‌درنگ نتیجه‌می‌شود، زیرا، به‌ازای هر $n \geq 1$، $K^{1/p} \subset K^{1/p^n} \subset K^{1/p^\infty}$.

(چهار) $\Rightarrow$ (یک) فرض کنیم $E = K(s_1, \ldots, s_n)$ و $\operatorname{tr.d.} E/K = r$. بنابرنتیجهٔ ۷.۱، $r \leq n$ و زیرمجموعه‌ای مـانند $\{s_1, \ldots, s_n\}$ یک پـایهٔ تعالی E روی K است؛ مثلاً "، $\{s_1, \ldots, s_r\}$. هرگاه $r = n$، آنگاه $\{s_1, \ldots, s_n\}$ یک پایهٔ تعالی جداگر است، که از آنجا (چهار) برقراراست. هرگاه $r < n$، آنگاه s_{r+1} روی $K(s_1, \ldots, s_r)$ جبری است (نتیجهٔ ۶.۱)؛ و لذا، ریشهٔ یک چندجمله‌ای تکین تحویل‌ناپذیر مانند

$$f(x) = \sum_{i=1}^{m} a_i x^i \in K(s_1, \ldots, s_r)[x]$$

است. "استدلال کوچکترین مخرج مشترک" نظیر آنکه در برهان قضیهٔ ۵.۱ به کار رفت نشان می‌دهد که $f(x) = d^{-1}\left(\sum_{i=1}^{m} v_i x^i\right)$، که‌درآن $0 \neq d \in K[s_1, \ldots, s_r]$، $v_i = h_i(s_1, \ldots, s_r)$ و $h_i \in K[x_1, \ldots, x_r]$. لذا، $f_1 = \sum_{i=0}^{m} h_i(x_1, \ldots, x_r) x_{r+1}^i \in K[x_1, \ldots, x_{r+1}]$ و

$$f_1(s_1, \ldots, s_r, s_{r+1}) = 0.$$

پس نتیجه می‌شودکه یک‌چندجمله‌ای مانند $g \in K[x_1, \ldots, x_{r+1}]$ از کوچکترین درجهٔ مثبت وجـود دارد بـه‌طوری‌که $g(s_1, \ldots, s_{r+1}) = 0$. واضـح اسـت که g در $K[x_1, \ldots, x_{r+1}]$ تحویل‌ناپذیر است. به یاد آورید که گوییم x_i در $g(x_1, \ldots, x_n)$ ظاهر می‌شود اگر جملهٔ ناصفری از g شامل عاملی از x_i^m با $m \geq 1$ باشد.

حکم می‌کنیم x_i ی در g با نمایی‌که بر p بخشپذیر نیست ظاهر می‌شود. در غیر این صورت، $g = c_0 + c_1 m_1(x_1, \ldots, x_{r+1})^p + \cdots + c_k m_k(x_1, \ldots, x_{r+1})^p$، که‌درآن $c_i \in K$، c_i ها همه صفر نیستند، و هر $m_j(x_1, \ldots, x_{r+1})$ یک تکجمله‌ای در $x_1, \ldots, x_{r+1}$ است. فرض کنیم $m_0(x_1, \ldots, x_{r+1}) = 1_K$ و، به‌ازای هر $j \geq 0$، $d_j \in K^{1/p}$ را طوری می‌گیریم که $d_j^p = c_j$. در این صورت، $g = \left(\sum_{j=0}^{k} d_j m_j(x_1, \ldots, x_{r+1})\right)^p$ و $g(s_1, \ldots, s_{r+1}) = 0$ ایجاب

می‌کند که

$$\sum_{j=0}^{k} d_j m_j(s_1, \ldots, s_{r+1}) = 0,$$

که از آنجا زیرمجموعهٔ $\{m_j(s_1, \ldots, s_{r+1}) \mid j \geq 0\}$ از F روی $K^{1/p}$ وابستهٔ خطی است. اما $\{m_j(s_1, \ldots, s_{r+1}) \mid j \geq 0\}$ لزوماً روی K مستقل خطی است (در غیر این صورت، یک $g_1 \in K[x_1, \ldots, x_{r+1}]$ با خاصیت $\deg g_1 < \deg g$ و $g_1(s_1, \ldots, s_{r+1}) = 0$ وجود می‌داشت). این امر با ازهم جدایی خطی F و $K^{1/p}$ تعارض دارد. بنابراین، x_i ی، مثلاً x_1، با نمایی که بر p بخشپذیر نیست در g ظاهر می‌شود.

چندجمله‌ای $g(x, s_2, \ldots, s_{r+1}) \in K(s_2, \ldots, s_{r+1})[x]$ لزوماً ناصفر است. در غیر این صورت، چون بنابر بند پیش x_1 در $g(x_1, \ldots, x_{r+1})$ ظاهر می‌شود، چندجمله‌ایی مانند $g_2 \in K[x_1, \ldots, x_{r+1}]$ به‌دست می‌آمد که $0 < \deg g_2 < \deg g$ و $g_2(s_1, s_2, \ldots, s_{r+1}) = 0$. یک چنین g_2 با انتخاب g متناقض است. بنابراین، $g(x, s_2, \ldots, s_{r+1}) \neq 0$. چون $g(s_1, s_2, \ldots, s_{r+1}) = 0$، s_1 روی $K(s_2, \ldots, s_{r+1})$ جبری است. اما $s_2, \ldots, s_{r+1}$ بوضوح روی $K(s_2, \ldots, s_{r+1})$ جبرینند و E روی $K(s_1, \ldots, s_{r+1})$ جبری می‌باشد. بنابر قضایای ۱۲.۱۰ V و ۱۳.۱۰ V، E روی $K(s_2, \ldots, s_{r+1})$ جبری است. چون $\text{tr.d.}E/K = r$، $\{s_2, \ldots, s_{r+1}\}$ یک پایهٔ تعالی E روی K است (نتیجهٔ ۷.۱).

برهان قضیهٔ ۲.۱ نشان می‌دهد که انتساب $x_i \mapsto s_i$ یک K ــ یکریختی مانند $\phi : K[x_2, \ldots, x_{r+1}] \cong K[s_2, \ldots, s_{r+1}]$ را معین می‌کند. واضح است که ϕ به یک K ــ یکریختی مانند $K[x_1, x_2, \ldots, x_{r+1}] = K[x_2, \ldots, x_{r+1}][x_1] \cong K[s_2, \ldots, s_{r+1}][x]$ توسیع می‌یابد به‌طوری که $x_1 \mapsto x$ و $g(x_1, \ldots, x_{r+1}) \mapsto g(x, s_2, \ldots, s_{r+1})$. چون ϕ یک یکریختی است، $g(x, s_2, \ldots, s_{r+1})$ باید در $K[s_2, \ldots, s_{r+1}][x]$ تحویل‌ناپذیر باشد. درنتیجه، بنابر لم III ۱۳.۶۰ و قضیهٔ III ۱۴.۶۰، $g(x, s_2, \ldots, s_{r+1})$ در $K[s_2, \ldots, s_{r+1}][x]$، و درنتیجه در $K(s_2, \ldots, s_{r+1})[x]$، تحویل‌ناپذیر است. چون ϕ یکریختی است، x باید با نمایی که بر p بخشپذیر نیست در $g(x, s_2, \ldots, s_{r+1})$ ظاهر شود. لذا، مشتق $g(x, s_2, \ldots, s_{r+1})$ ناصفر است (تمرین III ۳.۶۰)، که از آنجا، بنابر قضیهٔ III ۱۰.۶۰، $g(x, s_2, \ldots, s_{r+1})$ جدایی‌پذیر است. بنابراین، s_1 روی $K(s_2, \ldots, s_{r+1})$، و درنتیجه روی $K(s_2, \ldots, s_n)$، جبری جدایی‌پذیر می‌باشد. بخصوص، بنابر لم V ۶.۶۰، $E = K(s_1, \ldots, s_n)$ روی $K(s_2, \ldots, s_n)$ جبری جدایی‌پذیر است. لذا، هرگاه $\{s_2, \ldots, s_n\}$ یک پایهٔ تعالی E روی

K باشد، آنگاه E روی K به‌طور جدایی‌پذیر تولید شده است. اگر چنین نباشد، $\{s_2, \ldots, s_n\}$ شامل یک پایهٔ تعالی است (نتیجهٔ ۷.۱)، که می‌توان (پس از اندیسگذاری مجدد در صورت لزوم) آن را به صورت $\{s_2, \ldots, s_{r+1}\}$ فرض کرد. تکرار استدلال پیش (با s_{i+1} به جای s_i به‌ازای $i = 1, 2, \ldots, r+1$ و احتمالاً "اندیسگذاری مجدد") نشان می‌دهد که s_2 (و درنتیجه، $K(s_2, \ldots, s_n)$) روی $K(s_3, \ldots, s_n)$ جبری‌جدایی‌پذیراست. از اینرو، بنابر نتیجهٔ ۸.۶۰ V، E روی $K(s_3, \ldots, s_n)$ جبری جدایی‌پذیر است. با ادامهٔ این فرایند باید مآلاً "$s_1, \ldots, s_t$ یافت شوند به‌طوری‌که E روی $K(s_{t+1}, \ldots, s_n)$ جبری جدایی‌پذیر بوده و $\{s_{t+1}, \ldots, s_n\}$ یک پایهٔ تعالی E روی K باشد. بنابراین، E روی K به‌طور جدایی‌پذیر تولید شده است.

(سه) $\Rightarrow$ (چهار) فرض کنیم W زیرمجموعه‌ای متناهی از F باشدکه روی K مستقل خطی است. باید نشان داد که W روی K^{1/p^∞} مستقل خطی است. فرض کنیم $E = K(W)$. کافی است نشان دهیم که E و K^{1/p^∞} روی K ازهم جدای خطی‌اند، زیرا از این فورا" نتیجه می‌شود که W روی K^{1/p^∞} مستقل خطی است. چون W متناهی است، بنابر (چهار)، E دارای یک پایهٔ تعالی جداگر مانند S روی K است. با اعمال قضیهٔ ۴.۲ بر توسیعهای $K \subset K^{1/p^\infty}$ و $K \subset K(S) \subset E$ به‌صورت‌زیر، ثابت می‌کنیم E و K^{1/p^∞} ازهم جدای‌خطی‌اند. بنابرقضیهٔ ۷.۲، $K(S)$ و K^{1/p^∞} ازهم جدای خطی‌اند. فرض کنیم X زیرمجموعه‌ای از E باشد که روی $K(S)$ مستقل خطی است. چون E روی $K(S)$ جبری جدایی‌پذیر است، بنابرنیمی‌ازقضیهٔ ۸.۲ که‌قبلا" ثابت شد، X روی $K(S)^{1/p}$ مستقل خطی است. بنابراین، طبق لم ۶.۲، X^p روی $K(S)$ مستقل خطی است. سه جملهٔ اخیر قلب یک استدلال استقرایی را تشکیل می‌دهند که نشان می‌دهد که به‌ازای هر $m \geq 0$، X^{p^m} روی $K(S)$ مستقل خطی است (توجه کنید که $(X^{p^r})^p = X^{p^{r+1}}$). ازاینرو، بازبنابر لم ۶.۲، به‌ازای هر $m \geq 0$، X روی $K(S)^{1/p^m}$ مستقل‌خطی است. بنابراین، X روی $K(S)^{1/p^\infty}$ و در نتیجه روی زیر میدانش $K^{1/p^\infty}K(S)$ مستقل خطی است. پس ثابت کرده‌ایم که E و $K^{1/p^\infty}K(S)$ روی $K(S)$ ازهم‌جدای خطی‌اند. درنتیجه، بنابر قضیهٔ ۴.۲، E و K^{1/p^∞} روی K ازهم جدای خطی‌اند.

(پنج) $\Leftrightarrow$ (سه) کافی است ثابت کنیم $K_0 = K^{1/p^\infty}$. فرض‌کنیم $u \in K_0$. هرگاه u روی K متعالی باشد، آنگاه $v \in C$ ای‌وجود دارد که $v \neq u$ و v روی K متعالی است (مثلا"، $v = u^2$ را اختیار می‌کنیم). ترکیب $K(u) \cong K(x) \cong K(v)$ (که درآن یکریختیها به وسیلهٔ قضیهٔ ۵.۱۰ V داده شده‌اند) یک K ــ یکریختی مانند σ است به‌طوری‌که $\sigma(u) = v$.

لذا، داریم $1 = \text{tr.d.}K(x)/K = \text{tr.d.}K(u)/K = \text{tr.d.}K(v)/K$. قضیهٔ ۱۱۰۱ (و اگر $\text{tr.d.}C/K(u)$ نامتناهی باشد، لم ۸ . ۹ درآشنایی) ایجاب می‌کندکه $\text{tr.d.}C/K(u) = \text{tr.d.}C/K(v)$. بنابراین، طبق قضیهٔ ۱۲۰۱، σ به یک K ــ خودریختی C توسیع می‌یابد. اما $\sigma(u) = v \neq u$ ، که $u \in K_0$ رانقض می‌کند. بنابراین، u بایدروی K جبری‌باچندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ باشد. هرگاه $v \in C$ ریشهٔ دیگری‌از f باشد، آنگاه‌یک K ــ یکریختی مانند $\tau : K(u) \cong K(v)$ وجود دارد به‌طوری‌که $\tau(u) = v$ (نتیجهٔ ۹۰۱۰ V) . استدلالی مشابه‌حالت متعالی نشان می‌دهد که τ به یک K ــ خودریختی C توسیع می‌یابد. چون $u \in K_0$ ، باید داشته باشیم $u = \tau(u) = v$ ، که از آنجا f فقط‌یک ریشه در C دارد. لذا، u روی K صرفا" جدایی‌ناپذیر است. هرگاه $\text{char } K = 0$ ، آنگاه f (که لزوما" جدایی‌پذیر است) باید از درجهٔ 1 باشد. از اینرو، $u \in K = K^{1/\infty}$. هرگاه $\text{char } K = p \neq 0$ ، آنگاه، بنابر قضیهٔ ۴۰۶۰ V، به‌ازای $n \geq 0$ ی، $u^{p^n} \in K$. لذا، $u \in K^{1/p^n} \subset K^{1/p^\infty}$. پس ثابت کرده‌ایم که $K_0 \subset K^{1/p^\infty}$. به عکس، فرض کنیم $\text{char } K = p \neq 0$ ، $u \in K^{1/p^n} \subset K^{1/p^\infty}$ ، و $\sigma \in \text{Aut}_K C$. در این صورت، $\sigma(u)^{p^n} = \sigma(u^{p^n}) = u^{p^n}$ ، که از آنجا $\sigma(u)^{p^n} - u^{p^n} = (\sigma(u) - u)^{p^n} = 0$ و $\sigma(u) = u$. بنابراین، $K^{1/p^\infty} \subset K_0$.

تعریف ۱۱۰۲ . گوییم توسیع میدان F از میدان K روی K **جدایی‌پذیر** (یا یک **توسیع جدایی‌پذیر** از K) است اگر F در شرایط معادل قضیهٔ ۱۰۲ صدق کند.

چند تبصره. قضیهٔ ۸۰۲ نشان می‌دهد که این تعریف با استفادهٔ پیشین ما از واژهٔ "جدایی‌پذیر" درحالت توسیعهای جبری (تعریف ۱۰۳۰ V) سازگار است. چون شرط اول قضیهٔ ۱۰۲ وقتی $\text{char } K = 0$ بداهتا" برقرار است، هر توسیع میدان با مشخص 0 جدایی‌پذیر می‌باشد.

خواص اساسی جدایی‌پذیری در نتایج زیر از قضیهٔ ۱۰۲ آمده‌اند.

نتیجهٔ ۱۲۰۲ .(محک مک‌لین[1]) **هرگاه F یک توسیع میدان از میدان K بوده و F روی K به**

1. McLane

طور جدایی‌پذیر تولید شده باشد، آنگاه F روی K جدایی‌پذیر است. به‌عکس، هرگاه F روی K جدایی‌پذیر و با تولید متناهی باشد، مثلا $F = K(u_1, \ldots, u_n)$ *، آنگاه F روی K به‌طور جدایی‌پذیر تولید شده است. در واقع، زیرمجموعه‌ای از* $\{u_1, \ldots, u_n\}$ *یک پایهٔ تعالی جداگر F روی K می‌باشد.*

طرح برهان. برهان (یک) $\Rightarrow$ (سه) $\Rightarrow$ (چهار) در قضیهٔ ۱۰.۲ در اینجا به‌ازای $F = E$ معتبراست، زیرادر آن فقط از اینکه E به‌طورجدایی‌پذیر تولید شده است استفاده می‌شود. دو حکم اخیر نتایجی از برهان (چهار) $\Rightarrow$ (یک) در قضیهٔ ۱۰.۲ است.

نتیجهٔ ۱۳.۲. *فرض کنیم F یک توسیع میدان K بوده و E یک میدان میانی باشد.*
(یک) هرگاه F روی K جدایی‌پذیر باشد، آنگاه E روی K جدایی‌پذیر است.
(دو) هرگاه F روی E و E روی K جدایی‌پذیرباشد، آنگاه F روی K جدایی‌پذیراست.
(سه) هرگاه F روی K جدایی‌پذیرو E روی K جبری‌باشد، آنگاه F روی E جدایی‌پذیر است.

تبصره. (سه) در صورت جبری نبودن E روی K ممکن است درست نباشد (ر.ک. تمرین ۸).

طرح برهان ۱۳.۲. (دو) ازقضایای۴.۲و۱۰.۲استفاده‌کنید. اگر $\operatorname{char} K = p \neq 0$، فرض می‌کنیم X زیرمجموعه‌ای از F باشد که روی E مستقل خطی است. X را به پایهٔ U از F روی E توسیع داده و فرض می‌کنیم V پایه‌ای از E روی K باشد. برهان قضیهٔ IV ۱۶.۲۰ نشان می‌دهد که $UV = \{uv \mid u \in U, v \in V\}$ پایه‌ای از F روی K است، که از آنجا، بنابرجدایی‌پذیری، UV روی $K^{1/p}$ مستقل خطی است. لم ۶.۲ ایجاب می‌کندکه $(UV)^p = \{u^p v^p \mid u \in U, v \in V\}$ روی K مستقل خطی باشد. به علاوه، حکم می‌کنیم که V^p پایه‌ای از E روی K است. زیرا، بنابر (یک)، E روی K جدایی‌پذیر است. درنتیجه، ازهم‌جدایی خطی E و $K^{1/p}$ نشان می‌دهد که V روی $K^{1/p}$ مستقل خطی است، که از آنجا، طبق لم ۶.۲، V^p روی K مستقل خطی می‌باشد. چون بنابر نتیجهٔ ۹.۶۰ V، $E = KE^p$، V^p لزوما" E راروی K می‌پیماید. بنابراین، V^p پایه‌ای از E روی K است.

برای اتمام برهان باید نشان دهیم که X روی $E^{1/p}$ مستقل خطی است. هرگاه $\sum_i a_i u_i = 0$ $(a_i \in E^{1/p}; u_i \in X \subset U)$، آنگاه $\sum_i a_i^p u_i^p = 0$. چون هر $a_i^p \in E$ به شکل $\sum_j c_{ij} v_j^p$ $(c_{ij} \in K; v_j \in V)$ است، داریم $\sum_i (\sum_j c_{ij} v_j^p) u_i^p = \sum_{i,j} c_{ij} u_i^p v_j^p = 0$. استقلال خطی $(UV)^p$ ایجاب می‌کند که به‌ازای هر i,j، $c_{ij} = 0$؛ و درنتیجه، به‌ازای هر i، $a_i = 0$. بنابراین، X روی $E^{1/p}$ مستقل خطی است.

تمرینات

تذکر. E و F همواره توسیعهای میدانی از میدان K بوده، و C یک میدان به‌طور جبری بسته شامل E و F است.

۱. زیرحلقهٔ $E[F]$ به‌وسیلهٔ E تولید شده است و F یک فضای برداری روی K به‌طریق واضح است. حاصلضرب تانسوری $E \otimes_K F$ نیز یک K ــ فضای برداری است (ر.ک. قضیهٔ IV ۵۰۵۰ و نتیجهٔ IV ۱۲۰۵۰). E و F روی K ازهم جدای خطی‌اند اگر و فقط اگر K ــ تبدیل خطی $E \otimes_K F \to E[F]$ (که بر مولدهای $E \otimes_K F$ با $a \otimes b \mapsto ab$ داده شده است) یک یکریختی باشد.

۲. فرض کنید E و F به‌ترتیب میدانهای خارج‌قسمتی دامنه‌های صحیح R و S باشند. در این صورت، C یک R ــ مدول و یک S ــ مدول به طریق واضح است.

(آ) E و F روی K ازهم جدای خطی‌اند اگر و فقط اگر هر زیرمجموعهٔ R که روی K مستقل خطی است روی S نیز مستقل خطی باشد.

(ب) به علاوه، فرض کنید R یک فضای برداری روی K باشد. در این صورت، E و F روی K از هم‌جدای خطی‌اند اگر و فقط اگر هر پایهٔ R روی K روی F مستقل خطی باشد.

(پ) فرض کنید هر دوی R و S روی K فضاهای برداری باشند. در این صورت، E و F روی K ازهم جدای خطی‌اند اگر و فقط اگر به‌ازای هر پایهٔ X از R روی K و پایهٔ Y از S روی K، مجموعهٔ $\{uv \mid u \in X; v \in Y\}$ روی K مستقل خطی باشد.

۳. با استفاده از تمرین ۱، قضیهٔ ۲.۲ را ثابت کنید.

۴. با استفاده از تمرین ۱ و شرکتپذیری ضرب تانسوری، قضیهٔ ۴.۲ را ثابت کنید.

۵ . هرگاه $\operatorname{char} K = p \neq 0$ ، آنگاه

(آ) K^{1/p^n} به‌ازای هر $n \geq 0$ میدان است . ر.ک. تمرین III ۱۱.۱۰ ؛

(ب) K^{1/p^∞} یک میدان است ؛

(پ) K^{1/p^n} یک میدان تجزیه‌گر $\{x^{p^n} - k \mid k \in K\}$ روی K می‌باشد .

۶ . هرگاه $\{u_1, \ldots, u_n\}$ روی F مستقل جبری باشد ، آنگاه F و $K(u_1, \ldots, u_n)$ روی K ازهم جدای خطی‌اند .

۷ . هرگاه E یک توسیع صرفا" متعالی از K بوده و F روی K جبری باشد ، آنگاه E و F روی K ازهم جدای خطی‌اند .

۸ . فرض کنید $K = Z_p$ ، $F = Z_p(x)$ ، و $E = Z_p(x^p)$.

(آ) F روی K به‌طور جدایی‌پذیر تولید شده و جدایی‌پذیر است .

(ب) $E \neq F$.

(پ) F روی E جبری و صرفا" جدایی‌ناپذیر است .

(ت) $\{x^p\}$ یک پایهٔ تعالی F روی K است که یک پایهٔ تعالی جداگر نیست .

۹ . فرض کنید $\operatorname{char} K = p \neq 0$ و u روی K متعالی باشد . همچنین ، F روی K به وسیلهٔ $\{u, v_1, v_2, \ldots\}$ تولیدشده باشد که در آن ، به‌ازای $i = 1,2, \ldots$ ، r_i ریشه‌ای از $x^{p^i} - u \in K(u)[x]$ است . در این صورت ، F روی K جدایی‌پذیر است ، ولی F روی K به‌طور جدایی‌پذیر تولید شده نیست .

۱۰ . (آ) K یک میدان کامل است اگر و فقط اگر هر توسیع میدان K جدایی‌پذیر باشد (ر.ک. تمرین ۱۳.۶۰ V) .

(ب) (مک‌لین) فرض کنید K یک میدان کامل نبوده ، F کامل نباشد ، و $\operatorname{tr.d.} F/K = 1$. دراین صورت ، F روی K به‌طور جدایی‌پذیر تولید شده است .

۱۱ . F روی K صرفا" جدایی‌ناپذیر است اگر و فقط اگر K ــ تکریختی $F \to C$ نگاشت شمول باشد .

۱۲ . E و F روی K *آزاد* هستند اگر هر زیرمجموعهٔ X از E که روی K مستقل جبری است روی F نیز مستقل جبری باشد .

(آ) تعریف متقارن است (یعنی ، E و F روی K آزادند اگر و فقط اگر F و E روی K آزاد باشند) .

(ب) هرگاه E و F روی K ازهم‌جدای‌خطی باشند ، آنگاه E و F روی K آزادند .

با مثال نشان دهید که عکس مطلب درست نیست.

(پ) هرگاه E روی K جدایی‌پذیر بوده و E و F روی K آزاد باشند، آنگاه EF روی F جدایی‌پذیر است.

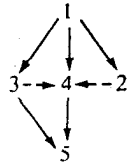
(ت) هرگاه E و F روی K آزاد بوده و هر دو روی K جدایی‌پذیر باشند، آنگاه EF روی K جدایی‌پذیر است.

۷

جبر خطی

جبر خطی ابزاری اصلی در بسیاری از شاخه‌های ریاضی است و کاربردهای گسترده‌ای دارد. بخش وسیعی از آن بررسی همریختیهای مدولهای آزاد (با تولید متناهی) (بویژه، تبدیلات خطی فضاهای برداری با بعد متناهی) است. بین این همریختیها و ماتریسها رابطهٔ مهمی وجود دارد (بخش ۱). بررسی رابطهٔ بین دو ماتریس که نمایش یک همریختی (نسبت به پایه‌های مختلف) اند ما را به مفاهیم تعادل و تشابه ماتریسها می‌رساند (بخشهای ۲ و ۴). بعضی از پایاهای مهم ماتریسها تحت تشابه در بخش ۵ مطرح می‌شوند. دترمینان ماتریسها (بخش ۳) در چند نقطه از بحث کاملا" مفید واقع می‌شود.

چون به کاربردهای جبر خطی علاقهٔ زیادی داریم، در این فصل مطالب زیادی با ماهیت محاسبه‌ای گنجانده شده است. برای بسیاری از خوانندگان وجود این مطالب به زحمتش می‌ارزد. با اینحال، فصل طوری تدوین یافته است که خوانندهٔ علاقه‌مند به مطالب اساسی و مهم نظریه بتواند آنها را در زمانی نسبتا" کوتاه فرا گیرد. کافی است نتایجی که نام حکم دارند را حذف کرده و به راهنماییهای شده در متن در اینکه چه مطالبی در آینده لازمند توجه نماید. ارتباط تقریبی بخشهای این فصل به قرار زیر است:



طبق معمول، سهم شکستهٔ $A \dashrightarrow B$ یعنی گاهی از نتایج بخش A در بخش B استفاده

می‌شود ، ولی بخش B اساسا" از بخش A مستقل است .

۱ ماتریسها و نگاشتها

خواص اساسی ماتریسها را به اختصار مرور می‌کنیم . سپس تمام روابط مهم بین ماتریسها و همریختیهای مدولهای آزاد را به دست می‌آوریم . جز در قضیهٔ ۱.۱ ، **همهٔ حلقه‌ها یکدار فرض می‌شوند** ، ولی قید دیگری را اعمال نمی‌کنیم . جز در بحث دوگانی در آخر بخش، همهٔ این مطالب تا پایان فصل لازم خواهند بود .

فرض کنیم R حلقه باشد . یک آرایه از عناصر به شکل

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2m} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm} \end{pmatrix}$$

که در آن $a_{ij} \in R$ ، n سطر (افقی) و m ستون (قائم) دارد ، یک **ماتریس $n \times m$** روی R نامیده می‌شود . ماتریس $n \times n$ یک **ماتریس مربعی** نام دارد . برای ساده بودن نماد ، معمولا" یک ماتریس دلخواه با حرف بزرگ A,B,C یا (a_{ij}) نموده می‌شود ،که‌مبین‌آن‌است که درایهٔ i-j م (سطر i ، ستون j) عنصر $a_{ij} \in R$ است. دو ماتریس $n \times m$ ، (a_{ij}) و (b_{ij}) **مساوی**‌اند اگروفقط اگر به‌ازای هر i,j ، در R ، $a_{ij} = b_{ij}$. گوییم عناصر $a_{11},a_{22},a_{33},\ldots$ **قطراصلی** ماتریس (a_{ij}) را تشکیل می‌دهند . هر ماتریس $n \times n$ که به‌ازای هر $i \neq j$ ، $a_{ij} = 0$ یک **ماتریس قطری** نام دارد . اگر R دارای واحد باشد ، **ماتریس‌همانی** I_n ماتریس قطری $n \times n$ است که درایه‌های قطر اصلی آن 1_R می‌باشند ؛ یعنی ، $I_n = (\delta_{ij})$ ،که‌درآن δ دلتای‌کرونکراست . ماتریسهای $n \times m$ که تمام درایه‌هایشان 0 است **ماتریسهای صفر** نام دارند . مجموعهٔ تمام ماتریسهای $n \times n$ روی R را با $\mathbf{Mat}_n R$ نشان می‌دهیم . **ترانهادهٔ** ماتریس $A = (a_{ij})$ ، $n \times m$ ماتریس $A^t = (b_{ij})$ ، $m \times n$ است (به اندازهٔ آن توجه کنید !) به‌طوری که به‌ازای هر i,j ، $b_{ij} = a_{ji}$.

هرگاه $A = (a_{ij})$ و $B = (b_{ij})$ ماتریسهای $n \times m$ می‌باشند،آنگاه **مجموع** $A + B$ ماتریس $n \times m$ می‌مانند (c_{ij}) تعریف می‌شود ،که‌درآن $c_{ij} = a_{ij} + b_{ij}$. هرگاه $A = (a_{ij})$ یک‌ماتریس $m \times n$ و $B = (b_{ij})$ یک ماتریس $n \times p$ باشد ، آنگاه **حاصلضرب** AB مساوی‌ماتریس

$m \times p$ ، (c_{ij}) تعریف می‌شود ،که‌درآن $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. ضرب در حالت کلی تعویضپذیر نیست . اگر $A = (a_{ij})$ یک ماتریس $n \times m$ بوده و $r \in R$ ، rA ماتریس $n \times m$ ، (ra_{ij}) و Ar ماتریس $n \times m$ ، $(a_{ij}r)$ است ؛ rI_n یک *ماتریس اسکالر* نام دارد .

هرگاه حاصلضرب ماتریسی AB تعریف شده باشد ، آنگاه حاصلضرب ماتریسهای ترانهادهٔ B^tA^t نیزتعریف شده است . هرگاه R تعویضپذیر باشد ، آنگاه $(AB)^t = B^tA^t$. این نتیجه درصورت تعویض‌ناپذیر بودن R ممکن است درست نباشد (تمرین ۱) .

قضیهٔ ۱۰۱ . *هرگاه R حلقه باشد ،آنگاه‌مجموعهٔ تمام‌ماتریسهای $n \times m$ روی R تحت جمع یک R-R دو مدول تشکیل می‌دهد ، که در آن ماتریس صفر $n \times m$ همانی جمعی می‌باشد .ضرب ماتریسها ،وقتی تعریف شده باشد ، شرکتپذیر و روی جمع پخشپذیر است . به‌ازای هر $n > 0$ ، Mat_nR حلقه است . اگر R یکدار باشد ، Mat_nR نیز یکدار است (یعنی ، ماتریس همانی I_n) .*

برهان . تمرین .

یکی از موارد استعمال مهم ماتریسها توصیف همریختیهای مدولهای آزاد است .

قضیهٔ ۲۰۱ . *فرض کنیم R حلقه‌ای‌یکدار باشد .همچنین ، E یک R ــ مدول چپ آزاد با پایه‌ای‌متناهی مرکب از n عنصر و F یک R ــ مدول چپ آزاد با پایه‌ای متناهی مرکب از m عنصرباشد . و نیز M ، R ــ مدول چپ تمام ماتریسهای $n \times m$ روی R باشد . در این صورت ، یک یکریختی گروههای آبلی مانند*

$$Hom_R(E,F) \cong M$$

وجود دارد . اگر R تعویضپذیر باشد ، این یک یکریختی R ــ مدولهای چپ می‌باشد .

برهان . فرض کنیم $\{u_1, \ldots, u_n\}$ پایه‌ای از E و $\{v_1, \ldots, v_m\}$ پایه‌ای از F بوده‌و $f \in \mathrm{Hom}_R(E,F)$. عناصری مانند r_{ij} از R وجود دارند به‌طوری‌که

$$f(u_1) = r_{11}v_1 + r_{12}v_2 + \cdots + r_{1m}v_m;$$

$$f(u_2) = r_{21}v_1 + r_{22}v_2 + \cdots + r_{2m}v_m;$$
$$\vdots$$
$$f(u_n) = r_{n1}v_1 + r_{n2}v_2 + \cdots + r_{nm}v_m.$$

r_{ij} ها به‌طور منحصر به فرد تعیین می‌شوند، زیرا $\{v_1, \ldots, v_m\}$ پایه‌ای از F است. نگاشت $\beta : \mathrm{Hom}_R(E,F) \to M$ را با $f \mapsto A$ تعریف می‌کنیم، که در آن A ماتریس $n \times m$ ، (r_{ij}) است. به‌آسانی تحقیق می‌شودکه β یک همریختی‌جمعی‌است. هرگاه $\beta(f) = 0$ ، آنگاه، به‌ازای هر عنصر پایهٔ u_i ، $f(u_i) = 0$ ، کهازآنجا $f = 0$.لذا، β یک تکریختی است. به‌ازای ماتریس $(r_{ij}) \in M$ ، $f : E \to F$ را با $f(u_i) = r_{i1}v_1 + r_{i2}v_2 + \cdots + r_{im}v_m$ $(i = 1,2, \ldots, n)$ تعریف می‌کنیم. چون E آزاد است، بنابر قضیهٔ IV ۱.۲۰ ، این f به عنوان عنصری از $\mathrm{Hom}_R(E,F)$ به‌طور منحصر به فرد معین است. بنابر ساخت، $\beta(f) = (r_{ij})$. بنابراین، β سورژکتیو، ودرنتیجه، یکریخت می‌باشد. هرگاه R تعویضپذیر باشد، آنگاه طبق تبصرهٔ بعد از قضیهٔ IV ۸.۴۰ ، $\mathrm{Hom}_R(E,F)$ یک R ــ مدول چپ با خاصیت $(rf)(x) = r(f(x))$ است. به آسانی تحقیق می‌شود که β یک یکریختی R ــ مدولهاست.

فرض کنیم R,E,F و β همانند درقضیهٔ ۲.۱ باشند. **ماتریس همریختی** $f \in \mathrm{Hom}_R(E,F)$ **نسبت به پایه‌های مرتب** $U = \{u_1, \ldots, u_n\}$ از E و $V = \{v_1, \ldots, v_m\}$ از F، مثل برهان قضیهٔ ۲.۱ ، ماتریس $n \times m$ ، $(r_{ij}) = \beta(f)$ است. لذا، سطر i م ماتریس f از ضرایب $f(u_i) \in F$ نسبت به پایهٔ مرتب $\{v_1, \ldots, v_m\}$ تشکیل شده است. در حالت خاص، وقتی $E = F$ و $U = V$ ، آن را **ماتریس درونریختی** f **نسبت به پایهٔ مرتب** U می‌نامیم.

تبصره. فرض کنیم E,F,f,U,V همانندبندپیش باشند. نقش یک عنصر دلخواه E تحت f را می‌توان به آسانی با ماتریس $A = (r_{ij})$ از f به صورت زیر حساب کرد. هرگاه $u = x_1u_1 + x_2u_2 + \cdots + x_nu_n \in E$ $(x_i \in R)$ ، آنگاه

$$f(u) = f\left(\sum_{i=1}^{n} x_iu_i\right) = \sum_{i=1}^{n} x_i f(u_i) = \sum_{i=1}^{n} x_i\left(\sum_{j=1}^{m} r_{ij}v_j\right)$$
$$= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} x_ir_{ij}\right)v_j = \sum_{j=1}^{m} y_jv_j,$$

که در آن $y_i = \sum_{j=1}^{n} x_j r_{ij}$. لذا ، هرگاه X ماتریس $1 \times n$ ، $(x_1\, x_2 \cdots x_n)$ و Y ماتریس $1 \times m$ ، $(y_1\, y_2 \cdots y_m)$ باشد ، آنگاه Y درست ماتریس حاصلضربی XA می‌باشد . X و Y را گاهی **بردارهای سطری** می‌نامند .

قضیهٔ ۳۰۱ . *فرض کنیم* R *حلقه‌ای یکدار بوده و* E,F,G ، R *ــ مدولهای چپ آزادی به ترتیب با پایه‌های مرتب متناهی* $U = \{u_1, \ldots, u_n\}$, $V = \{v_1, \ldots, v_m\}$, $W = \{w_1, \ldots, w_p\}$ *باشند . هرگاه* $f \in Hom_R(E,F)$ *دارای ماتریس* $n \times m$ ، A *(نسبت به پایه‌های* U و V *)* و $g \in Hom_R(F,G)$ *دارای ماتریس* $m \times p$ ، B *(نسبت به پایه‌های* V و W *) باشد ، آنگاه* $gf \in Hom_R(E,G)$ *دارای ماتریس* $n \times p$ ، AB *(نسبت به پایه‌های* U و W *) می‌باشد .*

برهان . هرگاه $A = (r_{ij})$ و $B = (s_{kj})$ ، آنگاه ، به‌ازای هر $i = 1,2, \ldots, n$ ،

$$gf(u_i) = g\left(\sum_{k=1}^{m} r_{ik} v_k\right) = \sum_{k=1}^{m} r_{ik} g(v_k) = \sum_{k=1}^{m} r_{ik}\left(\sum_{j=1}^{p} s_{kj} w_j\right)$$
$$= \sum_{j=1}^{p}\left(\sum_{k=1}^{m} r_{ik} s_{kj}\right) w_j .$$

بنابراین ، ماتریس gf نسبت به U و W دارای درایهٔ i-j م $\sum_{k=1}^{m} r_{ik} s_{kj}$ می‌باشد . اما این دقیقاً " درایهٔ i-j م ماتریس AB است .

فرض کنیم R حلقه‌ای یکدار بوده و E یک R ــ مدول چپ آزاد با پایهٔ متناهی U مرکب از n عنصر باشد . در این صورت ، $\mathrm{Hom}_R(E,E)$ حلقه‌ای یکدار است ، که در آن حاصلضرب نگاشتهای f و g همان تابع مرکب $fg : E \to E$ می‌باشد (تمرین IV ۷۰۱۰) . برای ارجاع در آینده، رابطهٔ بین حلقهٔ $\mathrm{Hom}_R(E,E)$ و حلقهٔ ماتریسی $\mathrm{Mat}_n R$ را ذکر می‌کنیم . هرگاه S و T حلقه باشند ، آنگاه گوییم تابع $\theta : S \to T$ یک **پادیکریختی** است اگر θ یک‌یکریختی **گروههای جمعی** باشد به‌طوری‌که به‌ازای هر $s_i \in S$ ، $\theta(s_1 s_2) = \theta(s_2)\theta(s_1)$. بنابر قضایای ۲۰۱ و ۳۰۱ ، نگاشت $\mathrm{Hom}_R(E,E) \to \mathrm{Mat}_n R$ که به هر $f \in \mathrm{Hom}_R(E,E)$ ماتریس آن (نسبت به U) را مربوط می‌کند یک پادیکریختی است . خوب می‌شد اگر $\mathrm{Hom}_R(E,E)$ با یک حلقهٔ ماتریسی یکریخت می‌شد . برای نشان دادن صحت این امر ، به مفهوم جدیدی

نیاز داریم .

هرگاه R حلقه باشد ، آنگاه **حلقهٔ متقابل** R ، که با R^{op} نموده می‌شود ، حلقه‌ای است‌که‌همان مجموعه عنصرهای R و همان‌جمع R را داشته ، و ضرب $\circ$ آن به صورت زیر تعریف شده باشد :

$$a \circ b = ba,$$

که در آن ba حاصل‌ضرب در R است (ر.ک. تمرین III ۱۷.۱۰) . نگاشت داده شده‌با $r \mapsto r$ بوضوح یک پادیکریختی $R \to R^{op}$ است . هرگاه $A = (a_{ij})$ و $B = (b_{ij})$ ماتریسهای $n \times n$ ی روی R باشند ،آنگاه A و B رامی‌توان ماتریسهایی روی R^{op} نیز درنظر گرفت .

توجه‌کنیدکه ، در $\mathrm{Mat}_n R$ ، $AB = (c_{ij})$ ، که در آن $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ ؛ اما در $\mathrm{Mat}_n R^{op}$ ، $AB = (d_{ij})$ ، که در آن

$$d_{ij} = \sum_{k=1}^{n} a_{ik} \circ b_{kj} = \sum_{k=1}^{n} b_{kj}a_{ik}.$$

قضیهٔ ۴.۱ . فرض کنیم R یک حلقه‌یکداربوده‌و E یک R ـ مدول چپ آزاد با پایه‌ای متناهی مرکب از n عنصر باشد . در این صورت ، یک یکریختی حلقه‌ها مانند

$$Hom_R(E,E) \cong Mat_n(R^{op})$$

وجوددارد . بخصوص،این یکریختی برای هر فضای برداری n بعدی E روی حلقهٔ بخشی R وجود دارد ، که در این حالت R^{op} نیز یک حلقهٔ بخشی است .

تبصره. اگر R تعویضپذیر باشد ، قضیهٔ ۴.۱ شکل زیباتری خواهد یافت ، زیرا در این صورت $R = R^{op}$.

طرح برهان ۴.۱ . فرض کنیم $\phi : \mathrm{Hom}_R(E,E) \to \mathrm{Mat}_n R$ یک پادیکریختی باشد که به هر نگاشت f ماتریس آن نسبت به پایهٔ داده شده را نسبت دهد . تحقیق کنید که نگاشت $\psi : \mathrm{Mat}_n R \to \mathrm{Mat}_n R^{op}$ داده شده با $\psi(A) = A^t$ یک پادیکریختی حلقه‌هاست . در این صورت ، نگاشت مرکب $\psi\phi : \mathrm{Hom}_R(E,E) \to \mathrm{Mat}_n R^{op}$ یک‌یکریختی‌حلقه‌هامی‌باشد . آخرین حکم قضیه نتیجه‌ای است از قضیهٔ ۴.۲۰ IV و تمرین ۷.۱۰ III .

فرض کنیم R حلقه‌ای یکدار بوده و $A \in \mathrm{Mat}_n R$. گوییم A **معکوسپذیر** یا **نامنفرد** است اگر $B \in \mathrm{Mat}_n R$ ای باشد به‌طوری‌که $AB = I_n = BA$. به آسانی معلوم می‌شود که **ماتریس معکوس** B ، در صورت وجود ، منحصر به فرد است؛ این ماتریس را معمولا" با A^{-1} نشان می‌دهیم . واضح است‌که $B = A^{-1}$ معکوسپذیر است و $(A^{-1})^{-1} = A$. حاصلضرب AC دو ماتریس معکوسپذیر معکوسپذیر است و $(AC)^{-1} = C^{-1}A^{-1}$. هرگاه A یک ماتریس معکوسپذیر روی یک حلقهٔ تعویضپذیر باشد ، آنگاه ترانهادهٔ آن نیز چنین است و $(A^t)^{-1} = (A^{-1})^t$ (تمرین ۱) .

واضح است‌که‌ماتریس‌یک همریختی R ــ مدولهای آزاد به انتخاب پایه‌های (مرتب) دردامنه و بردبستگی دارد . درنتیجه ، دانستن رابطهٔ بین ماتریسهایی که نگاشت یکسانی را نسبت به جفتهای مختلف از پایه‌های مرتب نمایش می‌دهند مفید می‌باشد .

لم ۵۰۱ . فرض کنیم R حلقه‌ای یکدار بوده و E,F ، R ــ مدولهای چپ آزادی به ترتیب با پایه‌های U,V می‌باشند به طوری‌که $|U| = n = |V|$. همچنین ، $A \in Mat_n R$. در این صورت ، A معکوسپذیر است اگرو فقط اگر A ماتریس یک یکریختی مانند $f: E \to F$ نسبت به U و V باشد . در این صورت ، A^{-1} ماتریس f^{-1} نسبت به V و U می‌باشد .

طرح برهان . همریختی R ــ مدولهای $f: E \to F$ یکریختی است‌اگرو فقط اگر یک‌همریختی R ــ مدولها مانند $f^{-1}: F \to E$ موجود باشد به‌طوری که $f^{-1}f = 1_E$ و $ff^{-1} = 1_F$ (ر.ک. قضیهٔ ۱ ۳۰۲۰) . فرض کنیم f یک یکریختی باماتریس A نسبت به U و V باشد . همچنین ، B ماتریس f^{-1} نسبت به V و U باشد . تصویر زیر را داریم :

$$\begin{array}{lccc} \text{نگاشت} : & & f & f^{-1} \\ \text{مدول} : & E & \longrightarrow F & \longrightarrow E \\ \text{پایه} : & U & V & U \\ \text{ماتریس} : & & A & B \end{array}$$

بنابر قضیهٔ ۳۰۱ ، AB ماتریس $f^{-1}f = 1_E$ نسبت به U است . اما I_n بوضوح ماتریس 1_E نسبت به U است . از اینرو ، بنابر برهان قضیهٔ ۲۰۱ ، $AB = I_n$. به همین نحو ، $BA = I_n$ ، که از آنجا A معکوسپذیر بوده و $B = A^{-1}$. استلزام عکس را به عنوان تمرین می‌گذاریم .

قضیهٔ ۶.۱ . *فرض کنیم* R *حلقه‌ای یکدار باشد . همچنین ،* E *و* F *،* R *ــ مدولهای چپ آزادی به‌ترتیب با پایه‌های مرتب متناهی* U *و* V *باشند به‌طوری‌که* $|U|=n,\ |V|=m$. *فرض کنیم* $f \in Hom_R(E,F)$ *دارای ماتریس* $n\times m$ ، A *نسبت به* U *و* V *باشد . در این صورت ، f نسبت به جفت دیگری از پایه‌های مرتب* E *و* F *دارای ماتریس* $n\times m$ ، B *است اگر و فقط اگر ، به‌ازای ماتریسهای معکوسپذیری چون* P *و* Q ، $B=PAQ$.

برهان . ($\Leftarrow$) هرگاه B ماتریس $n\times m$ ، f نسبت‌به‌پایه‌های U' از E و V' از F باشد ، آنگاه $n=|U'|$ و $m=|V'|$. فرض کنیم P ماتریس $n\times n$ نگاشت همانی 1_E نسبت به پایه‌های مرتب U' و U باشد . بنابرلم ۵.۱ ، P معکوسپذیر است . به همین نحو ، فرض کنیم Q ماتریس معکوسپذیر $m\times m$ ، 1_F نسبت‌به V و V' باشد (به‌ترتیب‌توجه کنید) . تصویر زیر را خواهیم داشت :

$$\begin{array}{lccccc} \text{نگاشت} : & 1_E & & f & & 1_F \\ \text{مدول} : & E & \longrightarrow & E & \longrightarrow & F & \longrightarrow & F \\ \text{پایه} : & U' & & U & & V & & V' \\ \text{ماتریس} : & & P & & A & & Q & \end{array}$$

بنابرقضیه ۳.۱ ، ماتریس $f=1_F f 1_E$ نسبت به U' و V' دقیقا " PAQ است . بنابراین ، طبق برهان ۲.۱ ، $B=PAQ$.

($\Rightarrow$) U,V,f,A طبق بالا هستند و $B=PAQ$ ، که در آن P و Q معکوسپذیرند . فرض کنیم $g:E\to E$ یکریختی با ماتریس P نسبت‌به U بوده و $h:F\to F$ یکریختی با ماتریس Q^{-1} نسبت به V باشد (لم ۵.۱) . هرگاه $U=\{u_1,\ldots,u_n\}$ ، آنگاه

$$g(U)=\{g(u_1),\ldots,g(u_n)\}$$

یک پایهٔ مرتب E نیزهست و P ماتریس 1_E نسبت‌به‌پایه‌های‌مرتب $g(U)$ و U می‌باشد . به همین نحو ، Q^{-1} ماتریس 1_F نسبت به پایه‌های مرتب $h(V)$ و V است ، که از آنجا $Q=(Q^{-1})^{-1}$ ماتریس 1_F نسبت به V و $h(V)$ می‌باشد (لم ۵.۱) . تصویر زیر را داریم

$$\begin{array}{lccccc} \text{نگاشت} : & 1_E & & f & & 1_F \\ \text{مدول} : & E & \longrightarrow & E & \longrightarrow & F & \longrightarrow & F \\ \text{پایه} : & g(U) & & U & & V & & h(V) \\ \text{ماتریس} : & & P & & A & & Q & \end{array}$$

بنابر قضیهٔ ۳.۱ ، ماتریس $f = 1_F f 1_E$ نسبت به پایه‌های مرتب $g(U)$ و $h(V)$ عبارت است از $PAQ = B$.

نتیجهٔ ۷.۱ . فرض کنیم R حلقه‌ای یکدار بوده و E یک R ــ مدول چپ آزاد با پایهٔ مرتب U به اصلیت متناهی n باشد . همچنین ، A ماتریس $n \times n$ ، $f \in Hom_R(E,E)$ نسبت به U باشد . در این صورت ، f دارای ماتریس $n \times n$ ، B نسبت به پایهٔ مرتب دیگر E است اگر و فقط اگر ، به‌ازای ماتریس معکوسپذیری چون P ، $B = PAP^{-1}$.

طرح برهان . هرگاه دربرهان قضیهٔ ۶.۱ $E = F$ ، $U = V$ ، و $U' = V'$ ، آنگاه ، بنابر لم ۵.۱ ، $Q = P^{-1}$.

نتایج فوق تعریف زیر را موجب می‌شوند .

تعریف ۸.۱ . فرض کنیم R حلقه‌ای یکدار باشد . گوییم دو ماتریس $A,B \in Mat_n R$ **متشابه**‌اند اگر یک ماتریس معکوسپذیر مانند P موجود باشد به‌طوری‌که $B = PAP^{-1}$. دو ماتریس $n \times m$ ، C,D را **معادل** گوییم اگر ماتریسهای معکوسپذیری چون P و Q موجود باشند به‌طوری‌که $D = PCQ$.

حال می‌توان قضیهٔ ۶.۱ و نتیجهٔ ۷.۱ را برحسب تعادل و تشابه بیان کرد . تعادل و تشابه روابطی هم‌ارزی‌اند (تمرین ۷) و به تفصیل در بخشهای ۲ و ۴ مورد مطالعه قرار خواهند گرفت .

این بخش را با بحثی از مدولهای راست و دوگانی به پایان می‌بریم .

هرگاه R تعویضپذیرباشد ،آنگاه‌نتایج پیشگفته‌برای R ــ مدولهای *راست* معتبرند . اما حالات مهمی وجود دارندکه در آنها R تعویضپذیر نیست (مثلا" ، فضاهای برداری روی یک حلقهٔ بخشی) . برای‌اثبات مشابه قضیهٔ ۳.۱ برای مدولهای راست در حالت غیر تعویضپذیری ، باید ماتریس یک همریختی را به صورتی دیگر تعریف کنیم .

فرض کنیم R حلقه‌ای یکدار بوده و E و F ، R ــ مدولهایی *راست* به ترتیب با پایه‌های مرتب متناهی $U = \{u_1, \ldots, u_n\}$ و $V = \{v_1, \ldots, v_m\}$ باشند . *ماتریس همریختی*

$f \in \mathrm{Hom}_R(E,F)$ نسبت به U و V را مساوی ماتریس $m \times n$ زیر تعریف می‌کنیم (به‌اندازهٔ آن توجه کنید):

$$\begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ s_{m1} & s_{m2} & \cdots & s_{mn} \end{pmatrix}$$

که در آن $s_{ij} \in R$ ها با معادلات

$$f(u_1) = v_1 s_{11} + v_2 s_{21} + v_3 s_{31} + \cdots + v_m s_{m1}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$f(u_n) = v_1 s_{1n} + v_2 s_{2n} + v_3 s_{3n} + \cdots + v_m s_{mn}$$

به‌طور منحصر به فرد معین می‌شوند. لذا، ضرایب $f(u_j)$ نسبت به پایهٔ مرتب V **ستون** j ام ماتریس $m \times n$ ، (s_{ij}) از f را تشکیل می‌دهند (با برهان قضیهٔ ۲۰۱ مقایسه کنید).

عمل f را می‌توان برحسب ماتریسها به صورت زیر توصیف کرد. فرض کنیم $u = u_1 x + u_2 x_2 + \cdots + u_n x_n$ $(x_i \in R)$ عنصری از E بوده و X ماتریس $n \times 1$ (یا **بردار ستونی**) $\begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$ باشد. همچنین، A ماتریس f نسبت به پایه‌های U و V باشد. در این صورت، $f(u) = v_1 y_1 + v_2 y_2 + \cdots + v_m y_m$ ، که در آن $y_i \in R$ و ماتریس $\begin{pmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_m \end{pmatrix}$

$m \times 1$ (بردار ستونی) AX است.

حال می‌توان مشابه نتایج ۲۰۱ تا ۵۰۱ در بالا را به آسانی ثابت کرد؛ بخصوص،

قضیهٔ ۹۰۱. *فرض کنیم R حلقه‌ای یکدار بوده و E,F ، R ـ مدولهای راست آزادی به ترتیب با پایه‌های متناهی U و V و به اصلیت n و m باشند. همچنین، N*

R ــ مدول راست تمام ماتریسهای $m \times n$ روی R باشد .

(یک) یک یکریختی گروههای آبلی مانند $Hom_R(E,F) \cong N$ وجود دارد که ، اگر R تعویضپذیر باشد ، یک یکریختی R ــ مدولهای راست می‌باشد ؛

(دو) فرض کنیم G یک R ــ مدول راست آزاد با پایهٔ متناهی W به اصلیت p باشد . هرگاه $f \in Hom_R(E,F)$ دارای ماتریس $m \times n$ ، A (نسبت به U و V) بوده و $g \in Hom_R(F,G)$ دارای ماتریس $p \times m$ ، B (نسبت به V و W) باشد ، آنگاه $gf \in Hom_R(E,G)$ دارای ماتریس $p \times n$ ، BA (نسبت به U و W) می‌باشد .

(سه) یک یکریختی حلقه‌ها مانند $Hom_R(E,E) \cong Mat_n R$ وجود دارد .

برهان. تمرین ؛ ر.ک. قضایای ۴۰۱ تا ۴۰۱ . توجه کنید که ، در مورد مدولهای راست ، (سه) درواقع یک یکریختی است تا یک پادیکریختی .

حکم ۱۰۰۱ . فرض کنیم R حلقه‌ای یکدار بوده و $f : E \to F$ یک همریختی R ــ مدولهای چپ آزاد با تولید متناهی باشد . هرگاه A ماتریس f نسبت به پایه‌های (مرتب) U و V باشد ، آنگاه A ماتریس همریختی دوگان $\bar{f} : F^* \to E^*$ از R ــ مدولهای راست آزاد نسبت به پایه‌های دوگان V^* و U^* نیز هست .

تبصره. نگاشتهای دوگان و پایه‌های دوگان در قضایای IV ۱۰۰۴۰ و IV ۱۱۰۴۰ تعریف شده‌اند . اگر R تعویضپذیر باشد (مثلا" ، میدان باشد) ، معمولا" دوگان M^* ، R ــ مدول چپ M را یک R ــ مدول چپ می‌گیرند (طبق معمول ، به‌ازای $r \in R, m^* \in M^*$ ، $rm^* = m^*r$) . دراین حالت ، ماتریس نگاشت دوگان $\bar{f}$ ترانهادهٔ A^t است (تمرین ۸) .

برهان ۱۰۰۱ . به یاد آوریدکه پایهٔ دوگان $V^* = \{v_1^*, \ldots, v_m^*\}$ از $F^* = \mathrm{Hom}_R(F,R)$ به‌وسیلهٔ

$$v_i^*(v_j) = \delta_{ij} \quad (1 \le i,j \le m \text{ ؛ دلتای کرونکر})$$

معین می‌شود ؛ و به همین ترتیب ، در مورد پایهٔ دوگان $U^* = \{u_1^*, \ldots, u_n^*\}$ از E^* (قضیهٔ IV ۱۱۰۴۰) . بنابر تعریف ماتریس یک نگاشت R ــ مدولها ، باید نشان دهیم که به‌ازای هر $j = 1,2, \ldots, m$ ، $\bar{f}(v_j^*) = \sum_{i=1}^{n} u_i^* r_{ij}$ ، که در آن $A = (r_{ij})$ ماتریس $n \times m$

از $f: E \to F$ نسبت به U و V می‌باشد. چون طرفین معادلهٔ فوق نگاشتهایی چون $E \to R$ می‌باشند، کافی است عمل آنها بر هر $u_k \in U$ امتحان شود. بنابر قضیهٔ IV ۱۰.۴۰، داریم

$$\bar{f}(v_j^*)(u_k) = v_j^*(f(u_k)) = v_j^*\left(\sum_{t=1}^{m} r_{kt}v_t\right) = \sum_{t=1}^{m} r_{kt}v_j^*(v_t) = r_{kj}.$$

از آن سو،

$$\left(\sum_{i=1}^{n} u_i^* r_{ij}\right)(u_k) = \sum_{i=1}^{n} u_i^*(u_k)r_{ij} = r_{kj}.$$

تمرینات

تذکر. فرض است که درایه‌های تمام ماتریسها در حلقهٔ یکدار R قرار دارند.

۱. فرض کنید R تعویضپذیر باشد.

(آ) هرگاه حاصلضرب ماتریسی AB تعریف شده باشد، آنگاه حاصلضرب B^tA^t نیز چنین است و $(AB)^t = B^tA^t$.

(ب) هرگاه A معکوسپذیر باشد، آنگاه A^t نیز چنین است و $(A^t)^{-1} = (A^{-1})^t$.

(پ) هرگاه R تعویضپذیر نباشد، آنگاه (آ) و (ب) ممکن است درست نباشد.

۲. گوییم ماتریس $(a_{ij}) \in \mathrm{Mat}_n R$

به‌ازای $j < i$، $a_{ij} = 0 \Leftrightarrow$ *(بالا)* **مثلثی** است

به‌ازای $j \leq i$، $a_{ij} = 0 \Leftrightarrow$ *اکیدا* **"مثلثی** است

ثابت کنید مجموعهٔ تمام ماتریسهای قطری زیرحلقه‌ای از $\mathrm{Mat}_n R$ است که (به‌عنوان حلقه) با $R \times \cdots \times R$ (n عامل) یکریخت است. نشان دهید که مجموعهٔ T مرکب از تمام ماتریسهای مثلثی زیرحلقه‌ای از $\mathrm{Mat}_n R$ است و مجموعهٔ I مرکب از تمام ماتریسهای اکیدا" مثلثی ایده‌آلی در T است. حلقهٔ خارج قسمتی T/I را مشخص کنید.

۳. (آ) مرکز حلقهٔ $\mathrm{Mat}_n R$ مرکب از تمام ماتریسها به شکل rI_n است، که در آن r در مرکز R است. [**راهنمایی.** هر ماتریس در مرکز $\mathrm{Mat}_n R$ با هر ماتریس $B_{r,s}$ تعویض‌می‌شود، که $B_{r,s}$ درموضع (r,s) دارای 1_R و در جاهای دیگر دارای 0 است.]

(ب) مرکز $\mathrm{Mat}_n R$ با مرکز R یکریخت است.

۴ . مجموعهٔ تمام ماتریسهای $m \times n$ روی R یک R ــ مدول آزاد با پایه‌ای مرکب از mn عنصر است .

۵ . ماتریس $A \in \mathrm{Mat}_n R$ **متقارن** است اگر $A = A^t$ و **متقارن اریب** است اگر $A = -A^t$.
(آ) هرگاه A و B متقارن [اریب] باشند ، آنگاه $A + B$ متقارن [اریب] است .
(ب) فرض کنید R تعویضپذیر باشد . هرگاه A,B متقارن باشند ، آنگاه AB متقارن است اگر و فقط اگر $AB = BA$. همچنین ، نشان دهید که به‌ازای هر ماتریس $B \in \mathrm{Mat}_n R$ ، BB^t و $B + B^t$ متقارن و $B - B^t$ متقارن اریب است .

۶ . هرگاه R یک حلقهٔ بخشی بوده و $A,B \in \mathrm{Mat}_n R$ چنان باشند که $BA = I_n$ ، آنگاه $AB = I_n$ و $B = A^{-1}$. [**راهنمایی .** از تبدیلات خطی استفاده کنید .]

۷ . تشابه ماتریسها رابطه‌ای هم‌ارزی بر $\mathrm{Mat}_n R$ است . تعادل ماتریسها رابطه‌ای هم‌ارزی بر مجموعهٔ تمام ماتریسهای $m \times n$ روی R است .

۸ . فرض کنید E,F فضاهای برداری (چپ) با بعد متناهی روی یک میدان بوده و فضاهای دوگان را فضاهای برداری چپ به طریق معمول بگیرید . هرگاه A ماتریس تبدیل خطی $f : E \to F$ باشد ، آنگاه A^t ماتریس نگاشت دوگان $\bar{f} : F^* \to E^*$ می‌باشد .

۲ رتبه و تعادل

هدف اصلی این بخش یافتن شرایط لازم و کافی برای تعادل ماتریسها روی یک حلقهٔ بخشی یا یک دامنهٔ ایده‌آل اصلی است . یک چنین شرط مستلزم مفهوم رتبه است . به علاوه ، برای این ماتریسها مجموعه‌های مفیدی از شکلهای کانونی عرضه می‌کنیم (قضیهٔ ۶۰۲ و حکم ۱۱۰۲) . بالاخره ، برای یافتن این شکلهای کانونی و برای محاسبهٔ معکوس یک ماتریس معکوسپذیر روی یک حلقهٔ بخشی تکنیکهایی عملی ارائه می‌دهیم . کاربردهای گروههای آبلی با تولید متناهی در ضمیمه ، که در آینده به کار نمی‌آید ، مطرح می‌شوند .

تعریف ۱۰۲ . فرض کنیم $f : E \to F$ یک تبدیل خطی از فضاهای برداری (چپ) روی حلقهٔ بخشی D باشد . **رتبهٔ** f بعد $\mathrm{Im}\, f$ و **پوچی** f بعد $\mathrm{Ker}\, f$ است .

تبصره . هرگاه $f : E \to F$ مثل تعریف ۱۰۲ باشد ، آنگاه ، طبق نتیجهٔ IV ۱۴۰۲۰ ،
$(\mathrm{rank}\, f) + (\mathrm{nullity}\, f) = \dim_D E$.

هرگاه R حلقه‌ای یکدار بوده و n عدد صحیح مثبتی باشد، آنگاه R^n، R ــ مدول آزاد $R \oplus \cdots \oplus R$ (n جمعوند) را نشان می‌دهد. **پایهٔ (مرتب) متعارف** R^n مرکب است از عناصر $\varepsilon_1 = (1_R, 0, \ldots, 0), \varepsilon_2 = (0, 1_R, 0, \ldots, 0), \ldots, \varepsilon_n = (0, \ldots, 0, 1_R)$.

تعریف ۲۰۲. *فضای سطری [فضای ستونی]* ماتریس A، $m \times n$ روی حلقهٔ یکدار R زیرمدول مدول چپ [راست] آزاد R^m [R^n] است که به‌وسیلهٔ سطرها [ستونهای] A به عنوان عناصری از R^m [R^n] تولید می‌شود. هرگاه R یک حلقهٔ بخشی باشد، آنگاه *رتبهٔ سطری [رتبهٔ ستونی]* A بعد فضای سطری [ستونی] A می‌باشد.

قضیهٔ ۳۰۲. *فرض کنیم $f : E \to F$ یک تبدیل خطی از فضاهای برداری چپ [راست] بابعد متناهی روی حلقهٔ بخشی D باشد. هرگاه A ماتریس f نسبت به جفتی از پایه‌های مرتب باشد، آنگاه رتبهٔ f مساوی رتبهٔ سطری [ستونی] A می‌باشد.*

تبصره. در رابطه با فضاهای برداری راست "رتبهٔ سطری" با "رتبهٔ ستونی" عوض می‌شود، واین به‌خاطرتعریف ماتریس یک نگاشت فضاهای برداری راست است (ص ۵۲۰).

برهان ۳۰۲. فرض کنیم A ماتریس $n \times m$ [$m \times n$]، f نسبت به پایه‌های مرتب $U = \{u_1, \ldots, u_n\}$ از E و $V = \{v_1, \ldots, v_m\}$ از F باشد. در این صورت، تحت یکریختی معمولی $F \cong D^m$ داده شده با $\sum_i r_i v_i \mapsto (r_1, \ldots, r_m)$، عناصر $f(u_1), \ldots, f(u_n)$ به روی سطرهای [ستونهای] A (به عنوان بردارهایی در D^m) نگاشته می‌شوند. چون $\operatorname{Im} f$ به وسیلهٔ $f(u_1), \ldots, f(u_n)$ پیموده می‌شود، $\operatorname{Im} f$ بافضای سطری [ستونی] A یکریخت است، که از آنجا رتبهٔ f مساوی رتبهٔ سطری [ستونی] A می‌باشد.

حال کمی از مطلب فاصله گرفته و ثابت می‌کنیم که رتبه‌های سطری و ستونی یک ماتریس روی یک حلقهٔ بخشی عملا" مساویند. این امر، که درنتیجهٔ ۵۰۲ ثابت شده است، برای درک مطالب آتی ضروری نیست، زیرا از حالا به بعد عملا" از "رتبهٔ سطری" استفاده می‌شود.

حکم ۴۰۲ . هر تبدیل خطی $f : E \to F$ از فضاهای برداری چپ با بعد متناهی روی حلقهٔ بخشی D همان رتبهٔ نگاشت دوگان آن $\bar{f} : F^* \to E^*$ را دارد .

نگاشت دوگان در قضیهٔ IV ۱۰۴۰ تعریف شده است .

برهان ۴۰۲ . فرض کنیم $\text{rank } f = r$. بنابر نتیجهٔ IV ۱۴۰۲۰ ، پایه‌ای مانند $X = \{u_1, \ldots, u_n\}$ وجود دارد بطوری‌که $\{u_{r+1}, \ldots, u_n\}$ پایه‌ای از $\text{Ker } f$ و $Y_1 = \{f(u_1), \ldots, f(u_r)\}$ پایه‌ای از $\text{Im } f$ است . Y_1 را به پایهٔ

$$Y = \{t_1 = f(u_1), \ldots, t_r = f(u_r), t_{r+1}, \ldots, t_m\}$$

از F توسیع می‌دهیم . پایه‌های دوگان X^* از E^* و Y^* از F^* را درنظر می‌گیریم (قضیهٔ IV ۱۱۰۴۰) . تحقیق کنید که به‌ازای هر $i = 1,2, \ldots, m$ ،

$$\bar{f}(t_i^*)(u_j) = t_i^*(f(u_j)) = \begin{cases} t_i^*(t_j) = \delta_{ij} & \text{اگر } j = 1,2, \ldots, r \text{ ،} \\ t_i^*(0) = 0 & \text{اگر } j = r+1, r+2, \ldots, n \text{ ،} \end{cases}$$

که در آن δ_{ij} دلتای کرونکر است . درنتیجه ، به‌ازای هر $j = 1, 2, \ldots, n$ ،

$$\bar{f}(t_i^*)(u_j) = \begin{cases} \delta_{ij} = u_i^*(u_j) & \text{اگر } i = 1,2, \ldots, r \text{ ،} \\ 0 & \text{اگر } i = r+1, r+2, \ldots, m \text{ ،} \end{cases}$$

بنابراین ، به‌ازای $i = 1,2, \ldots, r$ ، $\bar{f}(t_i^*) = u_i^*$ و ، به‌ازای $i = r+1, \ldots, m$ ، $\bar{f}(t_i^*) = 0$. $\text{Im } \bar{f}$ به وسیلهٔ $\bar{f}(Y^*)$ ، و درنتیجه به وسیلهٔ $\{u_1^*, \ldots, u_r^*\}$ ، پیموده می‌شود . چون $\{u_1^*, \ldots, u_r^*\}$ زیرمجموعه‌ای از X^* است ، در E^* مستقل خطی است . بنابراین ، $\{u_1^*, \ldots, u_r^*\}$ پایه‌ای از $\text{Im } \bar{f}$ است ، که از آنجا $\text{rank } \bar{f} = r = \text{rank } f$.

نتیجهٔ ۵۰۲ . هرگاه A یک ماتریس $m \times n$ روی حلقهٔ بخشی D باشد ، آنگاه رتبهٔ ستونی A = رتبهٔ سطری A .

برهان . فرض کنیم $f : D^n \to D^m$ یک تبدیل خطی فضاهای برداری چپ با ماتریس A نسبت به پایه‌های متعارف باشد . در این صورت ، نگاشت دوگان $\bar{f}$ از فضاهای برداری راست نیز دارای ماتریس A است (حکم ۱۰۰۱) . بنابر قضیهٔ ۳۰۲ و حکم ۴۰۲ ،

رتبهٔ ستونی A = رتبهٔ $\bar{f}$ = رتبهٔ f = رتبهٔ A .

تبصره. نتیجهٔ ۵.۲ فوراً نتیجه می‌دهد که، به‌ازای هر ماتریس A روی یک میدان، رتبهٔ سطری A^t = رتبهٔ سطری A.

به‌خاطر نتیجهٔ ۵.۲، از حالا به بعد صفات "سطری" و "ستونی" را حذف کرده و فقط می‌گوییم **رتبهٔ یک ماتریس** روی یک حلقهٔ بخشی.

درقضیهٔ ۶.۲ زیر، ماتریسهای‌معادل‌روی‌حلقهٔ‌بخشی D برحسب رتبه و ماتریسهای زیرتوصیف می‌شوند. هرگاه m,n اعداد صحیح مثبتی باشند، آنگاه $E_0^{n,m}$ مساوی ماتریس $n \times m$ صفرتعریف می‌شود. به‌ازای‌هر $(1 \leq r \leq \min(n,m))$ r، ماتریس $E_r^{n,m}$ ی $n \times m$ تعریف می‌شود که r سطر اول آن بردارهای پایهٔ متعارف $\varepsilon_1, \ldots, \varepsilon_r$ از D^m بوده و سایر سطرهای آن صفر می‌باشند:

$$E_r^{n,m} = \begin{pmatrix} 1_R & 0 & 0 & \cdots & 0 \\ 0 & 1_R & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & 0 & 1_R & 0 \cdots 0 \\ 0 & \cdots & 0 & 0 & 0 \cdots 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & & & 0 \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

واضح است که $\operatorname{rank} E_r^{n,m} = r$. به علاوه، هرگاه $E_r^{n,m}$ ماتریس همریختی $f: E \to F$ از R ـ مدولهای‌آزادنسبت‌به پایه‌های $\{u_1, \ldots, u_n\}$ از E و $\{v_1, \ldots, v_m\}$ از F باشد، آنگاه

$$f(u_i) = \begin{cases} v_i & \text{اگر } i = 1,2,\ldots,r \\ 0 & \text{اگر } i = r+1, r+2, \ldots, n \end{cases}$$

یک نتیجهٔ فوری قضیهٔ ۶.۱ و قضیهٔ ۶.۲ زیر این است که هر تبدیل خطی فضاهای برداری با بعد متناهی این شکل مناسب را به‌ازای جفتی‌از پایه‌ها خواهد داشت (تمرین ۶).

یک‌مجموعه‌از***شکلهای‌کانونی*** برای‌یک‌رابطهٔ هم‌ارزی R بر مجموعهٔ X زیرمجموعه‌ای مانند C از X است که از هر ردهٔ هم‌ارزی R درست یک عنصر دارد. به عبارت دیگر، به‌ازای هر $x \in X$، $c \in C$ ای‌منحصربه‌فرد وجود دارد به‌طوری که x تحت R با c هم‌ارز است. حال‌نشان می‌دهیم که ماتریسهای $E_r^{n,m}$ مجموعه‌ای از شکلهای کانونی برای رابطهٔ هم‌ارزی بر مجموعهٔ تمام ماتریسهای $n \times m$ روی یک حلقهٔ بخشی را تشکیل می‌دهد.

قضیهٔ ۶.۲ . فرض کنیم M مجموعهٔ تمام ماتریسهای $n \times m$ روی حلقهٔ بخشی D بوده و $A,B \in M$.

(یک) A **معادل** $E_r^{n,m}$ **است اگر و فقط اگر** $rank\ A = r$.

(دو) A **معادل** B **است اگر و فقط اگر** $rank\ A = rank\ B$.

(سه) ماتریسهای $E_r^{n,m}$ $(r = 1,2,\ldots, min\ (n,m))$ **مجموعه‌ای از شکلهای کانونی برای رابطهٔ هم‌ارزی بر** M **را تشکیل می‌دهند .**

طرح برهان . (یک) بنابر قضیهٔ ۲.۱ ، A ماتریس تبدیلی خطی مانند $f : D^n \to D^m$ نسبت بـه یک جفت پایه است . هرگاه $\text{rank } A = r$ ، آنگاه نتیجهٔ IV ۱۴.۲۰ ایجاب می‌کنـد کـه پایه‌هایی چون $U = \{u_1, \ldots, u_n\}$ از D^n و $V = \{v_1, \ldots, v_m\}$ از D^m وجود دارند به‌طوری‌که $f(u_i) = v_i$ به‌ازای $i = 1,2,\ldots,r$ و $f(u_i) = 0$ به‌ازای $i = r+1, \ldots, n$. واضح است‌که‌ماتریس f نسبت‌به U و V مساوی $E_r^{n,m}$ است . بنابراین ، طبق قضیهٔ ۶.۱ ، A معادل $E_r^{n,m}$ می‌باشد . به عکس، فرض کنیم A معادل $E_r^{n,m}$ باشد . بنابر قضیهٔ ۶.۱ ، یک تبدیل خطی مانند $g : D^n \to D^m$ هست به‌طوری که A ماتریس g نسبت به یک جفت پایه بوده و $E_r^{n,m}$ ماتریس g نسبت بـه جفت دیگری از پایه‌ها می‌باشد . درنتیجه ، طبق قضیهٔ ۳.۲ ، $\text{rank } A = \text{rank } g = \text{rank } E_r^{n,m} = r$. قسمتهای (دو) و (سه) نتایجی از (یک) هستند .

تعریف ، قضیه ، و نتـایج زیر ، علاوه بر روشهایی عملی برای ساختن ، چند پی‌آمد مفید دارند

(یک) شکلهای‌کانونی تحت تعادل برای ماتریسها روی یک دامنهٔ ایده‌آل اصلی (حکم ۱۱.۲) ؛

(دو) شکلهای کانونی $E_r^{n,m}$ تحت تعادل برای ماتریسها روی یک حلقهٔ بخشی ؛

(سه) معکوس یک ماتریس معکوسپذیر روی یک حلقهٔ بخشی (حکم ۱۲.۲) .

حکم ۱۱.۲ فقـط در بـرهان حکم ۹.۴ زیر به کار می‌رود . بقیهٔ مطالب از حکم ۱۱.۲ مستقل بوده و در آینده لازم نمی‌شوند .

ما اغلـب سطرهای [ستـونهای] یک ماتریس $n \times m$ روی حلقهٔ R را عناصر R^m [R^n] می‌گیریم . ماازجمع مضرب اسکالری از یک سطر [ستون] با دیگری سخن می‌گوییم ؛

مثلا " ،

$$r(a_1,a_2,\ldots,a_m)+(b_1,\ldots,b_m)=(ra_1+b_1,\ldots,ra_m+b_m).$$

تعریف ۷.۲ . فرض کنیم A ماتریسی روی حلقهٔ یکدار R باشد . هر یک از اعمال زیر یک *عمل سطری مقدماتی* بر A نام دارد :

(یک) تعویض دو سطر A باهم ؛

(دو) ضرب چپ یک سطر A در یکهٔ $c\varepsilon R$ ؛

(سه) به‌ازای $r\varepsilon R$ و $i\neq j$ ، جمع r برابر سطر j با سطر i .

اعمال ستونی مقدماتی بر A به طرز مشابه(به وسیلهٔ تعویض ضرب چپ در (دو) و (سه) با ضرب راست) تعریف می‌شوند . یک *ماتریس (تبدیل) مقدماتی* $n\times n$ ماتریسی است که با اعمال درست یک عمل سطری (ستونی) مقدماتی بر ماتریس همانی I_n به دست می‌آید .

قضیهٔ ۸.۲ . *فرض کنیم A یک ماتریس $n\times m$ روی حلقهٔ یکدار R بوده و* $[E_m]\ E_n$ *ماتریس مقدماتی حاصل از اعمال یک عمل سطری [ستونی] مقدماتی T بر* $I_n\ [I_m]$ *باشد . در این صورت ،* $E_nA\ [AE_m]$ *ماتریس حاصل از اعمال عمل T بر A می‌باشد .*

برهان . تمرین .

نتیجهٔ ۹.۲ . هر ماتریس مقدماتی $n\times n$ ، E روی حلقهٔ یکدار R معکوسپذیر بوده‌و معکوسش یک ماتریس مقدماتی است .

طرح برهان . تحقیق کنید که I_n را می‌توان از E با اعمال فقط یک عمل سطری مقدماتی T به‌دست‌آورد . هرگاه F ماتریس مقدماتی حاصل ازاعمال T بر I_n باشد ، آنگاه ، بنابر قضیهٔ ۸.۲ ، $FE=I_n$. مستقیما " تحقیق کنید که $EF=I_n$.

نتیجهٔ ۱۰.۲ . *هرگاه B ماتریس حاصل از ماتریس $n\times m$ ، A روی حلقهٔ یکدار R با اعمال دنباله‌ای متناهی از اعمال سطری و ستونی مقدماتی باشد ، آنگاه B معادل A خواهد بود.*

برهان. چون هر عمل سطری [ستونی] به کار رفته برای به دست آوردن B از A به وسیلهٔ ضرب چپ [راست] در یک ماتریس مقدماتی مناسب داده می‌شود (قضیهٔ ۸۰۲)، داریم $B = (E_p \cdots E_1)A(F_1 \cdots F_q) = PAQ$، که در آن هر E_i F_j یک ماتریس مقدماتی بوده و $P = E_p \cdots E_1$, $Q = F_1 \cdots F_q$. P و Q حاصلضربهایی از ماتریسهای معکوسپذیرند (نتیجهٔ ۹۰۲)؛ و درنتیجه، معکوسپذیر می‌باشند.

حال شکلهای کانونی تحت تعادل ماتریسها روی دامنهٔ ایده‌آل اصلی R را درنظر می‌گیریم. بنابرنتیجهٔ IV ۱۲۰۲۰، رتبهٔ یک مدول آزاد روی R یک پایای تعریف شده است. چون هر زیرمدول یک R ــ مدول آزاد آزاد است (قضیهٔ IV ۱۰۶۰)، می‌توان **رتبهٔ یک همریختی** $f : E \to F$ از R ــ مدولهای آزاد را رتبهٔ $\operatorname{Im} f$ تعریف کرد. به همین نحو، **رتبهٔ سطری ماتریس** A روی R مساوی رتبهٔ فضای سطری A تعریف می‌شود (ر.ک. تعریف ۲۰۲). به آسانی معلوم می‌شود که برهان قضیهٔ ۳۰۲ در اینجا معتبر است، که از آنجا رتبهٔ نگاشت f از R ــ مدولهای آزاد با تولید متناهی رتبهٔ سطری یک ماتریس f نسبت به جفتی از پایه‌ها می‌باشد. درنتیجه، هرگاه A معادل ماتریس B باشد، آنگاه رتبهٔ سطری B = رتبهٔ سطری A. زیرا، بنابر قضیهٔ ۶۰۱، A و B ماتریسهای یک همریختی $f : R^n \to R^m$ نسبت به جفتهای مختلفی از پایه‌هاست، که از آنجا رتبهٔ سطری B = رتبهٔ f = رتبهٔ سطری A. حال مشابه قضیهٔ ۶۰۲ برای ماتریسها روی یک دامنهٔ ایده‌آل اصلی را بیان می‌کنیم.

حکم ۱۱۰۲. *هرگاه A یک ماتریس $m \times n$ با رتبهٔ $r > 0$ روی یک دامنهٔ ایده‌آل اصلی باشد، آنگاه A معادل ماتریسی به شکل* $\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ *است، که در آن L یک ماتریس قطری $r \times r$ با درایه‌های قطری ناصفر $d_1, \ldots, d_r$ است به طوری که $d_1 \mid d_2 \mid \cdots \mid d_r$. ایده‌آلهای $(d_1), \ldots, (d_r)$ در R به طور منحصر به فرد به وسیلهٔ ردهٔ هم‌ارزی A معین می‌شوند.*

چند تبصره. این حکم مجموعه‌هایی از شکلهای کانونی برای رابطهٔ هم‌ارزی بر مجموعهٔ ماتریسهای $m \times n$ روی یک دامنهٔ ایده‌آل اصلی به دست می‌دهد (تمرین ۵). هرگاه R دامنهٔ اقلیدسی باشد، آنگاه برهان زیر همراه با تمرین ۷ و قضیهٔ ۸۰۲ نشان می‌دهد که

ماتریس $\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ را می‌توان از A با رشته‌ای متناهی از اعمال سطری و ستونی مقدماتی به دست آورد.

طرح برهان ۱۱.۲. (یک) به یاد آورید که $a,b \in R$ **باهم شریک** هستند اگر $a \mid b$ و $b \mid a$. بنابر قضیهٔ III ۲.۳۰، a و b شریکند اگر و فقط اگر $a = bu$ که در آن u یکه است. گوییم $c \in R$ یک **مقسوم‌علیه‌حقیقی** $a \in R$ است اگر $c \mid a$ و c یک شریک a نباشد (یعنی، $a \nmid c$). باسوءاستعمال زبان، گوییم دو مقسوم‌علیه حقیقی c_1 و c_2 از عنصر a **متمایزند** اگر c_1 و c_2 شریک نباشند. اما، طبق قضیهٔ III ۷.۳۰، R یک دامنهٔ یکتایی تجزیه است. هرگاه $a = p_1^{n_1}p_2^{n_2}\dots p_t^{n_t}$ (p_i ها تحویل‌ناپذیرومتمایزبوده و هر $n_i > 0$)، آنگاه هر مقسوم‌علیه a شریک‌عنصری به‌شکل $p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ است که، به‌ازای هر i، $0 \le k_i \le n_i$. درنتیجه، یک‌عنصرناصفر R فقط تعدادی‌متناهی مقسوم‌علیه‌حقیقی متمایز خواهد داشت.

(دو) اگر a و b عناصر ناصفری از R باشند، c را بزرگترین مقسوم‌علیه مشترک آنها می‌گیریم. بنابر تعریف III ۱۰.۳۰ و قضیهٔ III ۱۱.۳۰، $r,s \in R$ ی وجود دارند به طوری که $ar + bs = c$، $ca_1 = a$، و $cb_1 = b$، که از آنجا $a_1r + b_1s = 1_R$ و $ba_1 - ab_1 = 0$. درنتیجه، ماتریس $m \times m$

$$T = \begin{pmatrix} r & -b_1 & \\ s & a_1 & 0 \\ & 0 & I_{m-2} \end{pmatrix}$$

معکوسپذیر با معکوس

$$T^{-1} = \begin{pmatrix} a_1 & b_1 & \\ -s & r & 0 \\ & 0 & I_{m-2} \end{pmatrix}$$

می‌باشد. هرگاه سطر اول A مساوی $(a,b,a_{13},\dots,a_{1m})$ باشد، آنگاه A معادل $AT = I_nAT$ است، که سطر اولش مساوی $(c,0,a_{13},\dots,a_{1m})$ می‌باشد. هرگاه ستون اول[1] A مساوی

---

۱. برای راحتی درچاپ، اغلب یک بردار ستونی $n \times 1$ را به صورت ترانهادهٔ یک بردار سطری $1 \times n$ می‌نویسیم؛ مثلا "، $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = (a_1a_2)'$ ".

$(a,d,a_{31},\ldots,a_{n1})^t$ باشد، آنگاه روند مشابهی ماتریس معکوسپذیر S را به دست می‌دهد به‌طوری‌که A معادل SA بوده و SA دارای ستون اول $(e,0,a_{31},\ldots,a_{n1})^t$ می‌باشد، که در آن e بزرگترین مقسوم‌علیه مشترک a و d است. ماتریس S یا T یک **ماتریس ثانوی** نام دارد.

(سه) چون $A \neq 0$، رشته‌ای مناسب از تعویضهای سطری و ستونی و ضربهای راست در ماتریسهای ثانوی A را به ماتریس A_1 تغییر می‌دهد، که سطر اولش $(a_1,0,0,\ldots,0)$ با $a_1 \neq 0$ می‌باشد. بنابر قسمت (دو) و نتیجهٔ ۱۰.۲، A معادل A_1 است.

(چهار) هرگاه a_1 تمام درایه‌های ستون اول A_1 را عاد کند، آنگاه رشته‌ای متناهی از اعمال سطری مقدماتی ماتریس B به شکل زیر را تولید می‌کند؛

$$B = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2m} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix}$$

که، بنابر نتیجهٔ ۱۰.۲، معادل A_1، و لذا A، می‌باشد.

(پنج) هرگاه a_1 بعضی از درایه‌های ستون اول A_1 را عاد نکند، آنگاه رشته‌ای از تعویضهای سطری و ستونی و ضربهای چپ در ماتریسهای ثانوی A_1 را به ماتریس A_2 تغییر می‌دهند که دارای **ستون** اول $(a_2,0,0,\ldots,0)^t$ بوده و a_2 مقسوم‌علیه مشترک a_1 و b می‌باشد (ر.ک. قسمت (دو)). توجه کنید که A_2 ممکن است تعداد زیادی درایهٔ ناصفر در **سطر** اول داشته باشد. با اینحال، چون $a_2 \mid a_1$، $a_2 \mid b$، و $a_1 \nmid b$، بنابر (یک)، a_2 یک مقسوم‌علیه مشترک حقیقی a_1 است. بنابر (دو) و نتیجهٔ ۱۰.۲، A_2 معادل A_1 است.

(شش) هرگاه a_2 هر درایهٔ **سطر** اول A_2 را عاد کند، آنگاه رشته‌ای از اعمال ستونی مقدماتی ماتریسی تولید می‌کند که معادل A بوده و به همان شکل کلی B ی فوق است.

(هفت) هرگاه a_2 درایهٔ k در سطر اول A_2 را عاد نکند، آنگاه (سه) را تکرار کرده ماتریس A_3 را به‌دست می‌آوریم که معادل A بوده و دارای سطر اول $(a_3,0,0,\ldots,0)$ است، که در آن a_3 یک مقسوم‌علیه مشترک a_2 و k می‌باشد. A_3 ممکن است در ستون اول خود درایه‌های ناصفر داشته باشد. اما، چون $a_3 \mid a_2$، $a_3 \mid k$، و $a_2 \nmid k$، بنابر (یک)، a_3 یک مقسوم‌علیه حقیقی می‌باشد. به‌علاوه، بنابر (پنج)، a_2 و a_3 مقسوم‌علیه‌های حقیقی

متمایز a_1 اند. بنابر قسمت (دو) و نتیجهٔ ۶.۲.۱۰ ، A_3 معادل A_2 ، و درنتیجه معادل A ، می‌باشد.

(هشت) چون a_1 فقط تعدادی‌متناهی‌مقسوم علیه حقیقی متمایز دارد ، با چند بار تکرار (سه)تا (هفت) بایدماتریسی‌چون C به‌دست آید که معادل A بوده و به شکل زیر باشد :

$$C = \begin{pmatrix} s_1 & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2m} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix}$$

که در آن $s_1 \neq 0$.

(نه) اگر s_1 ، c_{ij} ای را عاد نکنـد ، سطر i را به سطر 1 افزوده و قسمتهای (سه) تا (هشت) را تکرارمی‌کنیم .نتیجه ماتریسی چون D است که با A معادل بوده و همان شکل کلی ماتریس C ی فوق رادارددودرایهٔ (1,1) آن عنصر s_2 است که یک مقسوم‌علیه مشترک s_1 و c_{ij} و یک مقسوم‌علیه حقیقی s_1 می‌باشد .

(ده) هرگاه s_2 هر درایهٔ D را عاد نکند ، آنگاه تکرار (نه) ماتریسی به دست می‌دهد که‌معادل A است ، همـان شکل کلی C را دارد ، و درایهٔ (1,1) آن s_3 است به‌طوری‌که s_3 یـک مقسـوم‌علیه حقیقـی s_2 می‌باشد ، که از آنجا s_2 و s_3 مقسوم‌علیه‌های حقیقی متمایز s_1 می‌باشند . چون s_1 فقط تعدادی متناهی مقسوم‌علیه حقیقی متمایز دارد ، تکرار چند بـارهٔ ایـن فرایند ماتریسی تولید می‌کند که معادل A است ، همان شکل کلی C را دارد ، و درایهٔ (1,1) آن تمام درایه‌های دیگر ماتریس را عاد می‌کند .

(یازده) با استفاده‌ازاستقرا و (ده) نشان‌دهیدکه A معادل‌ماتریس‌قطری $F = \begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ آمده در صورت‌قضیه است . چون رتبهٔ F بوضوح r است ، بنابر قضیهٔ ۶.۲ ، رتبهٔ A مساوی r می‌باشد .

(دوازده) (یکتایی) فرض‌کنیم A و F همانند در (یازده) باشند ، که $d_1, \ldots, d_r$ عناصر قطری L_r می‌باشند . فرض‌کنیم M ماتریسی معادل A باشد (درنتیجه ، $\operatorname{rank} M = r$) و N ماتریسی معادل M به شکل $\begin{pmatrix} L_r' & 0 \\ 0 & 0 \end{pmatrix}$ باشد ، که در آن L_r' یک ماتریس قطری $r \times r$ با

درایه‌های قطری ناصفر k_i است به‌طوری‌که $k_1 | k_2 | \cdots | k_r$. بنابرقضیهٔ ۲۰۱ ، F ماتریس یک همریختی مانند $f : R^m \to R^n$ نسبت به‌پایه‌های $\{u_1, \ldots, u_n\}$ از R^n و $\{v_1, \ldots, v_m\}$ از R^m است. درنتیجه ، $f(u_i) = d_i v_i$ به‌ازای $i = 1, 2, \ldots, r$ و $f(u_i) = 0$ به‌ازای $i = r+1, \ldots, n$ است ، که از آنجا $\operatorname{Im} f = Rd_1v_1 \oplus \cdots \oplus Rd_rv_r$. بنابر مشابه نتیجهٔ I ۱۱.۸۰ برای مدولها ،

$$R^m/\operatorname{Im} f \cong Rv_1/Rd_1v_1 \oplus \cdots \oplus Rv_r/Rd_rv_r \oplus Rv_{r+1} \oplus \cdots \oplus Rv_n \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R \oplus \cdots \oplus R$$

(m جمعوند ؛ $d_1 | d_2 | \cdots | d_r$) . چون طبق فرض F معادل N است ، قضیهٔ ۱.۶ ایجاب می‌کند که N ماتریس f نسبت به یک جفت متفاوت از پایه‌ها باشد . پس تکرار استدلال فوق نشان می‌دهد که $R^m/\operatorname{Im} f \cong R/(k_1) \oplus \cdots \oplus R/(k_r) \oplus R \oplus \cdots \oplus R$ (m جمعوند ؛ $k_1 | k_2 | \cdots | k_r$) . قضیهٔ ساختاری IV ۱۲.۶۰ برای مدولها روی یک دامنهٔ ایده‌آل اصلی ایجاب می‌کند که به‌ازای $i = 1, 2, \ldots, r$ ، $(d_i) = (k_i)$.

می‌توان با استفاده ازصورت ساده‌ای از تکنیکهای به کار رفته در برهان حکم ۱۱.۲ شکل کانونی $E_r^{n,m}$ از ماتریس $n \times m$ ، A روی حلقهٔ بخشی D را به دست آورد . اگر $A = 0 = E_0^{n,m}$ ، چیزی‌برای‌اثبات‌وجودندارد . هرگاه a_{ij} یک درایهٔ ناصفر در A باشد ، آنگاه تعویض سطرهای i و 1 و ستونهای j و 1 باهم a_{ij} را به موضع $(1,1)$ می‌برد . از ضرب سطر 1 در a_{ij}^{-1} ماتریسی به‌دست‌می‌آیدکه‌سطراولش به شکل $(1_R, c_2, \ldots, c_m)$ است . مضارب مناسبی از سطر 1 [ستون 1] را از هر سطر [ستون] بعدی کم کرده ، ماتریسی به شکل زیر به‌دست می‌آوریم :

$$\begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2m} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix}.$$

اگر هر $c_{ij} = 0$ ، کار تمام است . هرگاه $c_{ij} \neq 0$ ای ،آنگاه‌می‌توان‌روندبالارا بر زیرماتریس $(n-1) \times (m-1)$ ، (c_{ij}) تکرارکرد . چون اعمال سطری [ستونی] بر سطرهای $2, \ldots, n$ [ستونهای $2, \ldots, m$] بر سطر یا ستون اول اثری ندارند ، ماتریس زیر به دست می‌آید :

$$\begin{pmatrix} 1_R & 0 & 0 & \cdots & 0 \\ 0 & 1_R & 0 & \cdots & 0 \\ 0 & 0 & d_{33} & \cdots & d_{3m} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ 0 & 0 & d_{n3} & \cdots & d_{nm} \end{pmatrix}.$$

با ادامهٔ ایـن فـرایند مآلا" ماتریس $E_r^{n,m}$ معادل r ی به دست می‌آید. بنابر نتیجهٔ ۱۰۲، A معادل $E_r^{n,m}$ است، که‌از آنجا، بنابر قضیهٔ ۶۰۲، $r = \operatorname{rank} A$ و $E_r^{n,m}$ شکل کانونی A تحت هم‌ارزی است.

همانطورکه بـرهان حکم زیر نشان می‌دهد، صورت تعدیل یافتهٔ تکنیک فوق روشی ساختنی برای یافتن معکوس یک ماتریس معکوسپذیر است.

حکم ۱۲۰۲. *شرایط زیر بر ماتریس $n \times n$ A، روی حلقهٔ بخشی D باهم معادلند:*

(یک) $\operatorname{rank} A = n$؛

(دو) A *معادل ماتریس همانی* I_n *است*؛

(سه) A *معکوسپذیر است*؛

(چهار) A *حاصلضرب ماتریسهای تبدیل مقدماتی است.*

طرح برهان. بنابرقضیهٔ ۶۰۲، (دو) $\Leftrightarrow$ (یک)، زیرا $E_n^{n,n} = I_n$. (سه) $\Rightarrow$ (یک) سطرهای‌هرماتریس بارتبهٔ n لزوما" مستقل خطی‌اند (ر.ک. قضیهٔ ۵۰۲۰ IV و تعریف ۲۰۲.) درنتیجـه، سطر اول $A = (a_{ij})$ بردار صفر نبوده و، به‌ازای j ای، $a_{1j} \neq 0$. ستونهای j و 1 را باهم‌عوض‌کرده‌وستون جدید 1 را در a_{1j}^{-1} ضرب می‌کنیم. با تفریق مضارب مناسبی از ستون 1 از هر ستون پیش‌از آن، ماتریس زیر نتیجه می‌شود:

$$B = \begin{pmatrix} 1_D & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}.$$

بنابرنتیجهٔ ۱۰۲، B معادل A است. به استقرا فرض می‌کنیم رشته‌ای از اعمال ستونی

مقدماتی موجود باشد که A را به ماتریس (لزوماً "معادل")

$$C = \begin{pmatrix} & I_{k-1} & & 0 & \\ c_{k1} & \cdots & c_{kk} & \cdots & c_{kn} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ c_{n1} & \cdots & c_{nk} & \cdots & c_{nn} \end{pmatrix}$$

تغییر می‌دهد. به‌ازای $j \geq k$ ای، $c_{kj} \neq 0$، زیرا درغیر این صورت سطر k ترکیبی خطی از سطرهای $1, 2, \ldots, k-1$ خواهد بود. این، بنابر قضیهٔ ۶۰۲، با $\operatorname{rank} C = \operatorname{rank} A = n$ متناقض است. ستونهای j و k را باهم عوض‌کرده، ستون جدید k را در c_{kj}^{-1} ضرب نموده، و مضرب مناسبی از ستون k را از هر ستون $1, 2, \ldots, k-1$ و $k+1, \ldots, n$ کم می‌کنیم. نتیجه‌ماتریسی‌است مانند D که معادل A است (نتیجهٔ ۱۰۲):

$$D = \begin{pmatrix} & I_k & & 0 & \\ d_{k+1\,1} & \cdots & d_{k+1\,k+1} & \cdots & d_{k+1\,n} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ d_{n1} & \cdots & d_{n\,k+1} & \cdots & d_{nn} \end{pmatrix}.$$

این‌استقرا راتمام‌کرده‌و نشان می‌دهد که، وقتی $k = n$، A با رشته‌ای متناهی از اعمال **ستونی** مقدماتی به I_n تغییر می‌یابد. بنابراین، طبق قضیهٔ ۸۰۲، $A(F_1F_2\cdots F_t) = I_n$، که در آن هر F_i یک ماتریس مقدماتی است. بنابر تمرین ۷۰۱، ماتریس $F_1F_2\cdots F_t$ یک معکوس دوطرفهٔ A است، که از آنجا A معکوسپذیر است. نتیجهٔ ۹۰۲ و اینکه $A = F_t^{-1}\cdots F_2^{-1}F_1^{-1}$ نشان‌می‌دهندکه (چهار) $\Rightarrow$ (یک). بنابر لم ۵۰۱ و قضیهٔ ۳۰۲، (یک) $\Rightarrow$ (سه). بنابر نتیجهٔ ۹۰۲، (سه) $\Rightarrow$ (چهار).

تبصره. برهان (سه) $\Rightarrow$ (یک) نشان می‌دهد که $A^{-1} = F_1F_2\cdots F_t$ ماتریسی است که با همان رشته اعمال ستونی مقدماتی به کار رفته برای تغییر A به I_n بر I_n به دست می‌آید. به‌عنوان‌یک قاعده، این راه مناسبتری از به‌کارگیری دترمینانها برای محاسبهٔ معکوسهاست (بخش ۳).

ضمیمه: گروههای آبلی تعریف شده با مولدها و روابط

گوییم گروه آبلی G گروه آبلی تعریف شده با مولدهای $a_1, \ldots, a_m$ $(a_i \in G)$ و روابط

$$\begin{aligned} r_{11}a_1 + r_{12}a_2 + \cdots + r_{1m}a_m &= 0, \\ r_{21}a_1 + r_{22}a_2 + \cdots + r_{2m}a_m &= 0, \\ &\vdots \\ r_{n1}a_1 + r_{n2}a_2 + \cdots + r_{nm}a_m &= 0, \end{aligned}$$

$(r_{ij} \in \mathbf{Z})$ است مشروط بر اینکه $G \cong F/K$، که در آن F گروه آبلی آزاد بر مجموعهٔ $\{a_1, \ldots, a_m\}$ و K زیرگروه تولید شده به وسیلهٔ

$$b_1 = r_{11}a_1 + \cdots + r_{1m}a_m, b_2 = r_{21}a_1 + \cdots + r_{2m}a_m, \ldots, b_n = r_{n1}a_1 + \cdots + r_{nm}a_m$$

از F می‌باشد. توجه کنید که علامت a_i عنصری از گروه G و نیز یک عنصر پایهٔ گروه آبلی آزاد F را نمایش می‌دهد (ر.ک. قضیهٔ II ۱۰.۱۰). این تعریف با مفهوم مولدها و روابط که در بخش ۹.۱ مطرح شد سازگار است (ر.ک. تمرین ۱۰).

مسئلهٔ اصلی تعیین ساختار گروه آبلی G تعریف شده با مجموعهٔ متناهی داده شده از مولدها و روابط است. چون G با تولید متناهی است، G لزوماً یک مجموع مستقیم گروههای دوری است (قضیهٔ II ۱۰.۲۰). حال مرتبهٔ این جمعوندهای دوری را تعیین می‌کنیم.

فرض کنیم G گروه تعریف شده با مولدهای $a_1, \ldots, a_m$ و روابط $\sum_j r_{ij}a_j = 0$ به‌صورت فوق باشد. این وضع را با ماتریس $A = (r_{ij})$، $n \times m$ نشان می‌دهیم. سطرهای A مولدهای $b_1, \ldots, b_n$ زیرگروه K نسبت به پایهٔ مرتب $\{a_1, \ldots, a_m\}$ از F را نمایش می‌دهند. حکم می‌کنیم که اعمال سطری و ستونی مقدماتی وارد بر A اثر زیر را می‌گذارند.

(یک) هرگاه $B = (s_{ij})$ از A با یک عمل سطری مقدماتی به دست آمده باشد، آنگاه عناصر $c_1 = s_{11}a_1 + \cdots + s_{1m}a_m, \ldots, c_n = s_{n1}a_1 + \cdots + s_{nm}a_m$ از F (یعنی، سطرهای B) زیرگروه K را تولید می‌کند (ر.ک. تمرین 11 (آ)).

(دو) هرگاه $B = (s_{ij})$ از A با یک عمل ستونی مقدماتی به دست آمده باشد، آنگاه پایه‌ای از F مانند $\{a_1', \ldots, a_m'\}$ به آسانی به دست می‌آید که، به‌ازای هر i، $b_i = s_{i1}a_1' + s_{i2}a_2' + \cdots + s_{im}a_m'$ (تمرین 11 (ب)، (پ)).

هرگاه $K \neq 0$، آنگاه، بنابر حکم ۱۱.۲ و تمرین ۷، A را می‌توان با رشته‌ای متناهی از اعمال سطری و ستونی مقدماتی به ماتریس قطری زیر تغییر داد:

$$\begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & d_r & \\ & & & & 0 \\ & & 0 & & 0 \end{pmatrix}$$

به‌طوری‌که، به‌ازای هر i ، $d_i \neq 0$ و $d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_r$. به عبارت دیگر، با یک رشتهٔ متناهی از اعمال مقدماتی پایه‌ای از F مانند $\{u_1, \ldots, u_m\}$ دست می‌آید به‌طوری‌که $\{d_1u_1, d_2u_2, \ldots, d_ru_r\}$ ، K را تولید می‌کند. لذا، طبق نتیجهٔ I ۱۱.۸۰ ،

$$\begin{aligned} G \cong F/K &\cong (\mathbf{Z}u_1 \oplus \cdots \oplus \mathbf{Z}u_m)/(\mathbf{Z}d_1u_1 \oplus \cdots \oplus \mathbf{Z}d_ru_r \oplus 0 \oplus \cdots \oplus 0) \\ &\cong \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z}/0 \oplus \cdots \oplus \mathbf{Z}/0 \\ &\cong Z_{d_1} \oplus \cdots \oplus Z_{d_r} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}, \end{aligned}$$

که در آن رتبهٔ $(\mathbf{Z} \oplus \cdots \oplus \mathbf{Z})$ مساوی $m - r$ بوده و $d_1 \mid d_2 \mid \cdots \mid d_r$ (ر.ک. قضیهٔ II ۶.۲۰).

مثال. ساختار گروه آبلی G تعریف شده با مولدهای a,b,c و روابط $3a + 9b + 9c = 0$ و $9a - 3b + 9c = 0$ را تعیین می‌کنیم. فرض کنیم F گروه آبلی آزاد $\mathbf{Z}a + \mathbf{Z}b + \mathbf{Z}c$ و K زیرگروه تولید شده به وسیلهٔ $b_1 = 3a + 9b + 9c$ و $b_2 = 9a - 3b + 9c$ باشد. در این صورت، G با F/K یکریخت است و ماتریس

$$A = \begin{pmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{pmatrix}$$

را خواهیم داشت. ذیلا "مراحل مختلف قطری کردن ماتریس A به وسیلهٔ اعمال مقدماتی رانشان می‌دهیم (گاهی فقط در یک مرحله چند عمل انجام می‌شود). در هر مرحله پایهٔ F و مولدهای K نموده شده با ماتریس داده شده را ذکر می‌کنیم (این امر می‌تواند کمی پیچیده باشد؛ ر.ک. تمرین ۱۱).

ماتریس	پایهٔ مرتب F	مولدهای K که به صورت ترکیباتی خطی از این پایه بیان شده‌اند
$\begin{pmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{pmatrix}$	$a; b; c$	$b_1 = 3a + 9b + 9c$ $b_2 = 9a - 3b + 9c$
$\begin{pmatrix} 3 & 0 & 9 \\ 9 & -30 & 9 \end{pmatrix}$	$a + 3b; b; c$	$b_1 = 3(a + 3b) + 9c$ $b_2 = 9(a + 3b) - 30b + 9c$
$\begin{pmatrix} 3 & 0 & 0 \\ 9 & -30 & -18 \end{pmatrix}$	$a + 3b + 3c; b; c$	$b_1 = 3(a + 3b + 3c)$ $b_2 = 9(a + 3b + 3c) - 30b - 18c$
$\begin{pmatrix} 3 & 0 & 0 \\ 0 & -30 & -18 \end{pmatrix}$	$a + 3b + 3c; b; c$	$b_1 = 3(a + 3b + 3c)$ $b_2 - 3b_1 = -30b - 18c$
$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 18 & 30 \end{pmatrix}$	$a + 3b + 3c; c; b$	$b_1 = 3(a + 3b + 3c)$ $-(b_2 - 3b_1) = 18c + 30b$
$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 18 & 12 \end{pmatrix}$	$a + 3b + 3c; c + b; b$	$b_1 = 3(a + 3b + 3c)$ $-b_2 + 3b_1 = 18(c + b) + 12b$
$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 12 \end{pmatrix}$	$a + 3b + 3c; c + b;$ $b + (c + b)$	$b_1 = 3(a + 3b + 3c)$ $-b_2 + 3b_1 = 6(c + b) + 12(2b + c)$
$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$	$a + 3b + 3c; 5b + 3c;$ $2b + c$	$b_1 = 3(a + 3b + 3c)$ $-b_2 + 3b_1 = 6(5b + 3c)$

بنابراین، $G \cong F/K \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/0\mathbf{Z} \cong Z_3 \oplus Z_6 \oplus \mathbf{Z}$. هرگاه $\bar{v} \in G$ نقش $v + K \in F/K$ تحت یکریختی $F/K \cong G$ باشد، آنگاه G مجموع مستقیم داخلی یک زیرگروه دوری از مرتبهٔ سه با مولد $\overline{a + 3b + 3c}$، یک زیرگروه دوری از مرتبهٔ شش با مولد $\overline{5b + 3c}$، و یک زیرگروه دوری نامتناهی با مولد $\overline{2b + c}$ است.

تمرینات

۱. فرض کنید $f, g : E \to E$, $h : E \to F$, $k : F \to G$ تبدیلاتی خطی از فضاهای برداری چپ‌روی‌حلقهٔ‌بخشی D به ابعاد $\dim_D E = n$، $\dim_D F = m$، $\dim_D G = p$ باشد.

(آ) $\text{Rank}\,(f + g) \leq \text{rank}\, f + \text{rank}\, g$.

(ب) $\text{Rank}\,(kh) \leq \min\{\text{rank}\, h, \text{rank}\, k\}$.

(پ) $\text{Nullity}\, kh \leq \text{nullity}\, h + \text{nullity}\, k$.

(ت) $\text{Rank}\, f + \text{rank}\, g - n \leq \text{rank}\, fg \leq \min\{\text{rank}\, f, \text{rank}\, g\}$.

(ث) $\text{Max}\{\text{nullity}\, g, \text{nullity}\, h\} \leq \text{nullity}\, hg$

(ج) هرگاه $m \neq n$ ، آنگاه (ث) برای h و k نادرست است.

۲. ماتریس A ، $n \times m$ روی حلقهٔ بخشی D دارای معکوس چپ B ، $m \times n$ است (یعنی، $BA = I_m$) اگروفقط اگر $\operatorname{rank} A = m$. A دارای معکوس راست C ، $m \times n$ (با خاصیت $AC = I_n$) است اگر و فقط اگر $\operatorname{rank} A = n$.

۳. هرگاه $(c_{i1}, c_{i2}, \cdots c_{im})$ سطر ناصفری از ماتریس (c_{ij}) باشد، آنگاه ***درایهٔ پیشرو*** عبارت است از c_{it} ، که در آن t اولین عدد صحیحی است که $c_{it} \neq 0$. گوییم ماتریس $C = (c_{ij})$ روی حلقهٔ بخشی D به ***شکل سطری پلکانی تحویل یافته*** است اگر (یک) به‌ازای $r \geq 0$ ی، r سطر اول C (بردارهای سطری) ناصفر بوده و سایر سطرها صفر باشند؛ (دو) درایهٔ پیشرو هر سطر ناصفر 1_D باشد؛ (سه) هرگاه $c_{ij} = 1_D$ درایهٔ پیشرو سطر i باشد، آنگاه، به‌ازای هر $k \neq i$ ، $c_{kj} = 0$ ؛ (چهار) هرگاه $c_{1j_1}, c_{2j_2}, \ldots, c_{rj_r}$ درایه‌های پیشرو سطرهای $1, 2, \ldots, r$ باشند، آنگاه $j_1 < j_2 < \cdots < j_r$.

(آ) هرگاه C به شکل سطری پلکانی تحویل یافته باشد، آنگاه C تعداد سطرهای ناصفر است.

(ب) هرگاه A ماتریسی روی D باشد، آنگاه A را می‌توان با رشته‌ای متناهی از اعمال ***سطری*** مقدماتی به شکل سطری پلکانی تحویل یافته تغییر داد.

۴. (آ) دستگاه n معادلهٔ خطی از m مجهول x_i روی میدان K ی

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n \end{aligned}$$

دارای جواب (همزمان) است اگر و فقط اگر معادلهٔ ماتریسی $AX = B$ جوابی چون X داشته باشد، که A یک ماتریس $n \times m$ ، (a_{ij}) است، X یک بردار ستونی $m \times 1$ ، $(x_1 x_2 \cdots x_m)^t$ است، و B بردار ستونی $n \times 1$ ، $(b_1 b_2 \cdots b_n)^t$ می‌باشد.

(ب) هرگاه A_1, B_1 ماتریسهایی باشد که به ترتیب از A, B با اعمال رشتهٔ یکسانی از اعمال ***سطری*** مقدماتی بر هر دوی A_1 و B_1 به دست آمده‌اند، آنگاه X جواب $AX = B$ است اگر و فقط اگر X جواب $A_1X = B_1$ باشد.

(پ) فرض کنید C ماتریس $n \times (m+1)$

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} & b_1 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ a_{n1} & \cdots & a_{nm} & b_n \end{pmatrix}$$

باشد. در این صورت، $AX = B$ دارای جواب است اگر و فقط اگر $\operatorname{rank} A = \operatorname{rank} C$. در این حالت جواب منحصر به فرد است اگر و فقط اگر $\operatorname{rank} A = m$.

[**راهنمایی.** از (ب) و تمرین ۳ استفاده کنید.]

(ت) دستگاه $AX = B$ **همگن** است اگر B بردار ستونی صفر باشد. دستگاه همگن $AX = B$ دارای جواب نابدیهی است (یعنی، همهٔ x_i ها صفر نیستند) اگر و فقط اگر $\operatorname{rank} A < m$ (بخصوص، اگر $n < m$).

۵. فرض کنید R یک دامنهٔ ایده‌آل اصلی باشد. به‌ازای هر عدد صحیح مثبت r و دنبالهٔ $I_r \supset \cdots \supset I_2 \supset I_1$ از ایده‌آلهای ناصفر، دنبالهٔ $d_1, \ldots, d_r \in R$ را طوری اختیار کنید که $(d_i) = I_i$ و $d_1 \mid d_2 \mid \cdots \mid d_r$. به‌ازای جفت (n,m) از اعداد صحیح مثبت، فرض کنید S مجموعهٔ تمام ماتریسهای $n \times m$ به شکل $\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ باشد، که در آن $r = 1,2,\ldots,\min(n,m)$ و L_r یک ماتریس قطری $r \times r$ با قطر اصلی $d_1, \ldots, d_r$ است. نشان دهید S مجموعه‌ای از شکلهای کانونی تحت تعادل برای مجموعهٔ تمام ماتریسهای $n \times m$ روی R است.

۶. (آ) هرگاه $f : E \to F$ تبدیلی خطی از فضاهای برداری با بعد متناهی روی حلقهٔ بخشی باشد، آنگاه پایه‌ای چون $\{u_1, \ldots, u_n\}$ از E و $\{v_1, \ldots, v_m\}$ از F و عدد صحیح r $(r \leq \min(m,n))$ وجود دارند به‌طوری که به‌ازای $i = 1,2,\ldots,r$، $f(u_i) = v_i$ و به‌ازای $i = r+1, \ldots, n$، $f(u_i) = 0$.

(ب) نتیجه‌ای مشابه برای مدولهای آزاد با رتبهٔ متناهی روی یک دامنهٔ ایده‌آل اصلی بیان و اثبات کنید [ر.ک. حکم ۱۱.۲].

۷. فرض کنید R دامنه‌ای اقلیدسی با "تابع درجهٔ" $\phi : R - \{0\} \to \mathbf{N}$ باشد (تعریف III ۸.۳۰) (مثلاً "، فرض کنید $R = \mathbf{Z}$).

(آ) هرگاه $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ یک ماتریس 2×2 روی R باشد، آنگاه A را می‌توان با

رشته‌ای متناهی از اعمال سطری و ستونی مقدماتی به ماتریس قطری D تغییر داد. [**راهنمایی.** هرگاه $a \neq 0,\ b \neq 0$، آنگاه $b = aq + r$، که در آن $r = 0$، یا $r \neq 0$ و $\phi(r) < \phi(a)$. با استفاده از اعمال ستونی مقدماتی مناسب، نتیجه می‌شود که

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a & b - aq \\ c & d - cq \end{pmatrix} = \begin{pmatrix} a & r \\ c & * \end{pmatrix} \to \begin{pmatrix} r & a \\ * & c \end{pmatrix}.$$

چون $\phi(r) < \phi(a)$، تکرار این استدلال A را به $B = \begin{pmatrix} s & 0 \\ u & * \end{pmatrix}$ تغییر می‌دهد، که در آن $\phi(s) < \phi(a)$ اگر $s \neq 0$. اگر $u \neq 0$، استدلالی مشابه با سطرها B را به $C = \begin{pmatrix} t & w \\ 0 & * \end{pmatrix}$ تغییر می‌دهد، که در آن $\phi(t) < \phi(s) < \phi(a)$ اگر $t \neq 0$ (و احتمالاً $w \neq 0$). چون درجات درایه‌های $(1,1)$ اکیداً نزولی‌اند، تکرار این استدلالها پس از چند مرحله باید ماتریس قطری $D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ را به دست دهد.]

(ب) هرگاه A معکوسپذیر باشد، آنگاه A حاصلضربی از ماتریسهای مقدماتی است. [**راهنمایی.** بنابر قسمت (آ) و برهان نتیجهٔ ۲.۱۰، $D = PAQ$ که در آن P, Q معکوسپذیرند، که از آنجا D معکوسپذیر بوده و d_1, d_2 در R یکه‌اند. لذا، $A = P^{-1}\begin{pmatrix} d_1 & 0 \\ 0 & 1_R \end{pmatrix}\begin{pmatrix} 1_R & 0 \\ 0 & d_2 \end{pmatrix}Q^{-1}$؛ از نتیجهٔ ۲.۹ استفاده کنید.]

(پ) هر ماتریس ثانوی $n \times m$ (ر.ک. برهان حکم ۲.۱۱) روی یک دامنهٔ اقلیدسی حاصلضربی از ماتریسهای مقدماتی است.

۸. (آ) هر ماتریس معکوسپذیر روی یک دامنهٔ ایده‌آل اصلی حاصلضربی از ماتریسهای مقدماتی و ثانوی است.

(ب) هر ماتریس معکوسپذیر روی یک دامنهٔ اقلیدسی حاصلضربی از ماتریسهای مقدماتی است [ر.ک. تمرین ۷].

۹. فرض کنید $n_1, n_2, \ldots, n_t$، n عدد صحیح مثبت باشند به‌طوری‌که $n_1 + n_2 + \cdots + n_t = n$، و به‌ازای هر i، M_i یک ماتریس $n_i \times n_i$ باشد. همچنین، M ماتریس $n \times n$

$$\begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_t \end{pmatrix}$$

باشد، که در آن قطر اصلی هر M_i بر قطر اصلی M قرار دارد. به‌ازای هر جایگشت σ از $\{1,2,\ldots,t\}$، M با ماتریس

$$\sigma M = \begin{pmatrix} M_{\sigma 1} & & & 0 \\ & M_{\sigma 2} & & \\ & & \ddots & \\ 0 & & & M_{\sigma t} \end{pmatrix}$$

متشابه است. [**راهنمایی.** هرگاه $t = 3$، $\sigma = (13)$، و $P = \begin{pmatrix} 0 & & I_{n_3} \\ & I_{n_2} & \\ I_{n_1} & & 0 \end{pmatrix}$، آنگاه $P^{-1} = \begin{pmatrix} 0 & & I_{n_1} \\ & I_{n_2} & \\ I_{n_3} & & 0 \end{pmatrix}$ و $PMP^{-1} = \sigma M$. در حالت کلی، از برهان نتایج ۸۰۲ تا ۱۰۲ تقلید کنید.]

۱۰. مجموعهٔ $\{a_1,\ldots,a_n\}$ و کلمات $w_1,w_2,\ldots,w_r$ (بر a_i) داده‌شده‌اند. فرض کنید F^* گروه (ضربی غیرآبلی) آزاد روی مجموعهٔ $\{a_1,\ldots,a_n\}$ بوده و M زیرگروه نرمال تولید شده به وسیلهٔ کلمات $w_1,w_2,\ldots,w_r$ باشد (ر.ک. بخش I ۹۰). همچنین، N زیرگروه نرمال تولید شده به وسیلهٔ تمام کلمات به شکل $a_ia_ja_i^{-1}a_j^{-1}$ باشد.

(آ) F^*/M گروه تعریف شده به وسیلهٔ مولدهای $\{a_1,\ldots,a_n\}$ و روابط $\{w_1 = w_2 = \cdots = w_r = e\}$ است (تعریف I ۴۰۹۰).

(ب) F^*/N گروه آبلی آزاد بر $\{a_1,\ldots,a_n\}$ است (ر.ک. تمرین II ۱۲۰۱۰).

(پ) $F^*/(M \vee N)$ (با نماد ضربی) گروه آبلی تعریف شده به وسیلهٔ مولدهای $\{a_1,\ldots,a_n\}$ و روابط $\{w_1 = w_2 = \cdots = w_r = e\}$ است (ر.ک. ص ۵۳۷).

(ت) بروریختیهای گروههای $F^* \to F^*/N \to F^*/(M \vee N)$ وجود دارند.

۱۱ . فرض‌کنید F یک‌گروه‌آبلی آزادبا پایهٔ $\{a_1, \ldots, a_m\}$ باشد . همچنین ، K زیرگروهی از F باشد که به وسیلهٔ $b_1 = r_{11}a_1 + \cdots + r_{1m}a_m, \ldots, b_n = r_{n1}a_1 + \cdots + r_{nm}a_m$ $(r_{ij} \in \mathbf{Z})$ تولید می‌شود .

(آ) به‌ازای هر i ، هر دوی $\{b_1, \ldots, b_{i-1}, -b_i, b_{i+1}, \ldots, b_n\}$ و

$$\{b_1, \ldots, b_{i-1}, b_i + rb_j, b_{i+1}, \ldots, b_n\}$$

$(r \in \mathbf{Z};\ i \neq j)$ ، K را تولید می‌کنند . [ر.ک. لم II ۵۰۱۰]

(ب) به‌ازای هر i ، $\{a_1, \ldots, a_{i-1}, -a_i, a_{i+1}, \ldots, a_n\}$ پایه‌ای از F است که نسبت به آن $b_j = r_{j1}a_1 + \cdots + r_{j,i-1}a_{i-1} - r_{ji}(-a_i) + r_{j,i+1}a_{i+1} + \cdots + r_{jm}a_m$.

(پ) به‌ازای هر i و $j \neq i$ ، $\{a_1, \ldots, a_{j-1}, a_j - ra_i, a_{j+1}, \ldots, a_m\}$ $(r \in \mathbf{Z})$ پایه‌ای از F است که نسبت به آن

$$b_k = r_{k1}a_1 + \cdots + r_{k,i-1}a_{i-1} + (r_{ki} + rr_{kj})a_i + r_{k,i+1}a_{i+1} + \cdots + r_{k,j-1}a_{j-1} + r_{kj}(a_j - ra_i) + r_{k,j+1}a_{j+1} + \cdots + r_{km}a_m.$$

۱۲ . ساختار گروه آبلی G تعریف شده با مولدهای $\{a,b\}$ و روابط $2a + 4b = 0$ و $3b = 0$ را تعیین کنید . همین کار را در مورد گروه با مولدهای $\{a,b,c,d\}$ و روابط $2a + 3b = 4a = 5c + 11d = 0$ و برای گروه با مولدهای $\{a,b,c,d,e\}$ و روابط

$$\{a - 7b + 14d - 21c = 0;\ 5a - 7b - 2c + 10d - 15e = 0;\ 3a - 3b - 2c + 6d - 9e = 0;\ a - b + 2d - 3e = 0\}$$

انجام دهید .

۳ دترمینانها

تابع دترمینان $\mathrm{Mat}_n R \to R$ را به عنوان نوع خاصی از تابع R ــ چندخطی تعریف کرده و خواص مقدماتی آن را عرضه می‌کنیم (قضیهٔ ۵۰۳) . بقیهٔ بخش به تکنیکهای محاسبهٔ دترمینانها و رابطهٔ بین دترمینانها و معکوسپذیری اختصاص دارد . این مطالب ، جز معدودی ، در آینده لازم نخواهند شد . سراسر این بخش *تمام حلقه‌ها تعویضپذیر و یکدار بوده و همهٔ مدولها یکانی هستند* .

اگر B یک R ــ مدول بوده و $n \geq 1$ عددی صحیح باشد ، B^n ، R ــ مدول $B \oplus B \oplus \cdots \oplus B$ (n جمعوند) است . البته ، مجموعهٔ زمینهٔ مدول B^n چیزی جز حاصلضرب دکارتی $B \times \cdots \times B$ نیست .

تعریف ۱۰۳ . فرض کنیم $B_1, \ldots, B_n$ و C مدولهایی روی حلقهٔ تعویضپذیر و یکدار R باشند. گوییم تابع $f : B_1 \times \cdots \times B_n \to C$ ، **R ــ چندخطی** است اگر به‌ازای هر $i = 1,2, \ldots, n$ و هر $r,s \in R$ ، $b_i \in B_i$ ، و $b,b' \in B_i$ ،

$$f(b_1, \ldots, b_{i-1}, rb + sb', b_{i+1}, \ldots, b_n) = rf(b_1, \ldots, b_{i-1}, b, b_{i+1}, \ldots, b_n) + sf(b_1, \ldots, b_{i-1}, b', b_{i+1}, \ldots, b_n).$$

هرگاه $C = R$ ، آنگاه f یک **فرم n ــ خطی** یا **R ــ چندخطی** نامیده می‌شود. هرگاه $C = R$ و $B_1 = B_2 = \cdots = B_n = B$ ، آنگاه f یک **فرم R ــ چندخطی بر B** نام دارد.

توابع 2 ــ خطی را معمولاً **دوخطی** می‌نامند (ر.ک. قضیهٔ IV ۶.۵۰). فرض کنیم B و C ، R ــ مدول بوده و $f : B^n \to C$ یک تابع R ــ چندخطی باشد. گوییم f **متقارن** است اگر

به‌ازای هر جایگشت $\sigma \in S_n$ ، $f(b_{\sigma 1}, \ldots, b_{\sigma n}) = f(b_1, \ldots, b_n)$

و **متقارن اریب** است اگر

به‌ازای هر $\sigma \in S_n$ ، $f(b_{\sigma 1}, \ldots, b_{\sigma n}) = (\operatorname{sgn} \sigma) f(b_1, \ldots, b_n)$.

گوییم f **متناوب** است اگر

هر وقت به‌ازای $i \neq j$ ای ، $b_i = b_j$ ، داشته باشیم $f(b_1, \ldots, b_n) = 0$.

مثال . فرض کنیم B ، R ــ مدول $R \oplus R$ بوده و $d : B \times B \to R$ با

$$((a_{11},a_{12}),(a_{21},a_{22})) \mapsto a_{11}a_{22} - a_{12}a_{21}$$

تعریف شده باشد. d یک فرم دوخطی متناوب متقارن اریب بر B است. هرگاه عناصر B را به صورت سطرهای ماتریسهای 2×2 روی R تصور کنیم ، آنگاه d چیزی جز تابع دترمینان معمولی نخواهد بود.

قضیهٔ ۲۰۳ . *هرگاه B و C مدولهایی روی حلقهٔ تعویضپذیر یکدار R باشند ، آنگاه هر تابع R ــ چندخطی متناوب $f : B^n \to C$ متقارن اریب است.*

طرح برهان . در حالت خاص وقتی $n = 2$ و $\sigma = (1\ 2)$ ، داریم

$$0 = f(b_1 + b_2, b_1 + b_2) = f(b_1,b_1) + f(b_1,b_2) + f(b_2,b_1) + f(b_2,b_2)$$

$$= 0 + f(b_1,b_2) + f(b_2,b_1) + 0,$$

که از آنجا $f(b_2,b_1) = -f(b_1,b_2) = (\operatorname{sgn}\sigma) f(b_1,b_2)$. درحالت کلی ، نشان دهید که کافی است σ یک‌ترانهش فرض‌شود . دراین‌صورت ، برهان تعمیم آسانی از حالت $n = 2$ است .

توجه اصلی ما به فرمهای n ــ خطی متناوب بر R ــ مدول آزاد R^n است . این گونه فرم تابعی است از $(R^n)^n = R^n \oplus \cdots \oplus R^n$ (n جمعوند) به R .

قضیهٔ ۳.۳ . هرگاه R حلقه‌ای تعویضپذیر و یکدار بوده و $r \in R$ ، آنگاه یک فرم R ــ چندخطی متناوب منحصر به فرد مانند $f : (R^n)^n \to R$ وجود دارد به‌طوری‌که $f(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n) = r$ ، که در آن $\{\varepsilon_1,\ldots,\varepsilon_n\}$ پایهٔ متعارف R^n است .

تبصره . پایهٔ متعارف بعدازتعریف ۱.۲ تعریف شد . مطلب زیر ممکن است به فهم برهان کمک نماید . چون عناصر R^n را می‌توان با بردارهای سطری $1 \times n$ یکی کرد ، لذا واضح است که یک یکریختی R ــ مدولها مانند $(R^n)^n \cong \operatorname{Mat}_n R$ وجوددارد که با $(X_1,X_2,\ldots,X_n) \mapsto A$ داده می‌شود ، که در آن A ماتریسی با سطرهای $X_1,X_2,\ldots,X_n$ است . هرگاه $\{\varepsilon_1,\ldots,\varepsilon_n\}$ پایهٔ متعارف R^n باشد ،آنگاه ، تحت این یکریختی ، $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n) \mapsto I_n$. لذا ، فرم چند خطی f قضیهٔ ۳.۳ را می‌توان تابعی تصور کرد که n شناسه‌اش سطرهای ماتریسهای $n \times n$ اند .

برهان ۳.۳ (یکتایی) . هرگاه یک چنین فرم n ــ خطی متناوب f موجود بوده و $(X_1,\ldots,X_n) \in (R^n)^n$ ، آنگاه ، به‌ازای هر i ، $a_{ij} \in R$ ای وجود دارد به‌طوری‌که $X_i = (a_{i1},a_{i2},\ldots,a_{in}) = \sum_{j=1}^{n} a_{ij}\varepsilon_j$ ، $(R^n)^n \cong \operatorname{Mat}_n R$ (به عبارت دیگر ، تحت یکریختی $(X_1,\ldots,X_n) \mapsto (a_{ij})$) . لذا ، طبق چندخطی بودن ،

$$\begin{aligned} f(X_1,\ldots,X_n) &= f\Big(\sum_{j_1} a_{1j_1}\varepsilon_{j_1}, \sum_{j_2} a_{2j_2}\varepsilon_{j_2}, \ldots, \sum_{j_n} a_{nj_n}\varepsilon_{j_n}\Big) \\ &= \sum_{j_1}\sum_{j_2}\cdots\sum_{j_n} a_{1j_1}a_{2j_2}\cdots a_{nj_n} f(\varepsilon_{j_1},\varepsilon_{j_2},\ldots,\varepsilon_{j_n}). \end{aligned}$$

چون f متناوب است ، تنها جملات ناصفر ممکن در مجموع نهایی آنهایی هستند که در

آنها همهٔ $j_1, j_2, \ldots, j_n$ متمایزند؛ یعنی، $\{j_1, \ldots, j_n\}$ چیزی جز مجموعهٔ $\{1,2,\ldots,n\}$ نیست؛ درنتیجه، به‌ازای $\sigma \in S_n$ ای، $(j_1, \ldots, j_n) = (\sigma 1, \ldots, \sigma n)$. لذا، بنابر قضیهٔ ۲۰۳،

$$\begin{aligned} f(X_1, \ldots, X_n) &= \sum_{\sigma \in S_n} a_{1\sigma 1} a_{2\sigma 2} \cdots a_{n\sigma n} f(\varepsilon_{\sigma 1}, \varepsilon_{\sigma 2}, \ldots, \varepsilon_{\sigma n}) \\ &= \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma 1} \cdots a_{n\sigma n} f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n). \end{aligned}$$

چون $f(\varepsilon_1, \ldots, \varepsilon_n) = r$، داریم

$$f(X_1, \ldots, X_n) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) r a_{1\sigma 1} a_{2\sigma 2} \cdots a_{n\sigma n}. \qquad (1)$$

معادلهٔ (۱) نشان می‌دهد که $f(X_1, \ldots, X_n)$ به‌طور منحصر به‌فرد با $X_1, \ldots, X_n$ و r معین می‌شود.

(وجود) کافی است تابع $f : (R^n)^n \to R$ را با فرمول (۱) تعریف کنید (که در آن $X_i = (a_{i1}, \ldots, a_{in})$) و تحقیق کنید f یک فرم n ــ خطی متناوب با خاصیت $f(\varepsilon_1, \ldots, \varepsilon_n) = r$ است. چون به‌ازای هر k ثابت، هر جمعوند $\sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) r a_{1\sigma 1} \cdots a_{n\sigma n}$ درست شامل یک عامل a_{ij} با $i = k$ است، به‌آسانی معلوم می‌شود که f یک R ــ چندخطی است. چون $\varepsilon_i = \sum_{j=1}^{n} \delta_{ij} \varepsilon_j$ (دلتای کرونکر)، $f(\varepsilon_1, \ldots, \varepsilon_n) = r$. بالاخره، باید نشان دهیم که اگر $X_i = X_j$ و $i \neq j$، $f(X_1, \ldots, X_n) = 0$. برای ساده بودن نماها، فرض می‌کنیم $i = 1, j = 2$. هرگاه $\rho = (12)$، آنگاه‌نگاشت $A_n \to S_n$ داده‌شده با $\sigma \mapsto \sigma\rho$ یک تابع انژکتیو است که نقش آن مجموعهٔ تمام جایگشتهای فرد می‌باشد (زیرا σ ی زوج فرد بودن $\sigma\rho$ را ایجاب می‌کند و $|A_n| = |S_n|/2$). لذا، S_n اجتماع جفتهای دو به دو ازهم جدای $\{\sigma, \sigma\rho\}$ است که $\sigma \in A_n$. هرگاه σ زوج باشد، آنگاه جمعوند $f(X_1, X_1, X_3, \ldots, X_n)$ نظیر به σ مساوی است با

$$+ r a_{1\sigma 1} a_{2\sigma 2} a_{3\sigma 3} \cdots a_{n\sigma n}.$$

چون $X_1 = X_2$، $a_{1\sigma 1} = a_{2\sigma 1}$ و $a_{2\sigma 2} = a_{1\sigma 2}$، درنتیجه جمعوند نظیر به جایگشت فرد $\sigma\rho$ عبارت است از

$$\begin{aligned} -r a_{1\sigma\rho 1} a_{2\sigma\rho 2} a_{3\sigma\rho 3} \cdots a_{n\sigma\rho n} &= -r a_{1\sigma 2} a_{2\sigma 1} a_{3\sigma 3} \cdots a_{n\sigma n} \\ &= -r a_{1\sigma 1} a_{2\sigma 2} a_{3\sigma 3} \cdots a_{n\sigma n}. \end{aligned}$$

لذا، جمعوندهای $f(X_1,X_1,X_3,\ldots,X_n)$ دو به دو حذف شده و

$$f(X_1,X_1,X_3,\ldots,X_n)=0.$$

بنابراین، f متناوب می‌باشد.

حال می‌توان با استفاده از قضیهٔ ۳.۳ و تبصرهٔ بعد از آن، دترمینانها را تعریف کرد. بخصوص، اغلب $\mathrm{Mat}_n R$ و $(R^n)^n$ را تحت یکریختی (مذکور در تبصره)، که با $(\varepsilon_1,\ldots,\varepsilon_n)\mapsto I_n$ داده می‌شود، یکی خواهیم کرد. درنتیجه، هر فرم **چندخطی بر** $\mathbf{Mat}_n\mathbf{R}$ یک فرم R ــ چندخطی بر $(R^n)^n$ است که شناسه‌هایش سطرهای ماتریسهای $n\times n$ اند که عناصری از R^n گرفته شده‌اند.

تعریف ۴.۳. فرض کنیم R یک حلقهٔ تعویضپذیر و یکدار باشد. فرم R ــ چندخطی متناوب منحصر به فرد $d: Mat_n R\to R$ با خاصیت $d(I_n)=1_R$ **تابع دترمینان** بر $Mat_n R$ نام دارد. **دترمینان** ماتریس $A\in Mat_n R$ عنصر $d(A)\in R$ است و با $|A|$ نموده می‌شود.

قضیهٔ ۵.۳. *فرض کنیم R حلقهٔ تعویضپذیر و یکدار بوده و* $A,B\in Mat_n R$.
(یک) هر فرم R ــ چندخطی متناوب f بر $Mat_n R$ مضرب اسکالر منحصر به فردی از تابع دترمینان d است.

(دو) هرگاه $A=(a_{ij})$، آنگاه $|A|=\sum_{\sigma\in S_n}(sgn\ \sigma)a_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}$.

(سه) $|AB|=|A||B|$.

(چهار) هرگاه A در $Mat_n R$ معکوسپذیر باشد، آنگاه $|A|$ در R یکه است.

(پنج) هرگاه A و B متشابه باشند، آنگاه $|A|=|B|$.

(شش) $|A^t|=|A|$.

(هفت) هرگاه $A=(a_{ij})$ مثلثی باشد، آنگاه $|A|=a_{11}a_{22}\cdots a_{nn}$:

(هشت) هرگاه B از تعویض دو سطر [ستون] A با هم به دست آمده باشد، آنگاه $|B|=-|A|$. هرگاه B از ضرب یک سطر [ستون] A در $r\in R$ به دست آمده باشد، آنگاه $|B|=r|A|$. هرگاه B با افزودن مضرب اسکالری از سطر i [ستون i] به سطر j [ستون] $(i\neq j)$ به دست آمده باشد، آنگاه $|B|=|A|$.

طرح برهان. (یک) فرض کنیم $f(I_n) = r \in R$. همچنین، d تابع دترمینان باشد. تحقیق کنید تابع $rd : \mathrm{Mat}_n R \to R$ داده‌شده با $A \mapsto r|A| = rd(A)$ نیز یک فرم R ــ چند خطی متناوب بر $\mathrm{Mat}_n R$ است به‌طوری‌که $rd(I_n) = r$، که‌ازآنجا، طبق حکم یکتایی قضیهٔ ۳.۳، $f = rd$. یکتایی r بی‌درنگ نتیجه می‌شود.

(دو) چیزی جز بیان مجدد معادلهٔ (۱) در برهان قضیهٔ ۳.۳ نیست. (سه) فرض کنیم B ثابت بوده و *ستونهای* B را با $Y_1, Y_2, \ldots, Y_n$ نشان می‌دهیم. هرگاه C یک ماتریس $n \times m$ با *سطرهای* $X_1, \ldots, X_n$ باشد، آنگاه درایهٔ (i,j) ی CB دقیقاً "عنصر $(X_iY_1, X_iY_2, \ldots, X_iY_n)$ ی 1×1 ماتریس X_iY_j است. لذا، سطر i م CB مساوی است. با استفاده از این امر، تحقیق کنید که نگاشت $\mathrm{Mat}_n R \to R$ داده شده با $C \mapsto |CB|$ یک فرم R ــ چند خطی متناوب مانند f بر $\mathrm{Mat}_n R$ است. بنابر (یک)، به‌ازای $r \in R$ ی، $f = rd$. درنتیجه، $|CB| = f(C) = rd(C) = r|C|$. بخصوص، $|B| = |I_n B| = r|I_n| = r$، که‌ازآنجا $|AB| = r|A| = |A||B|$.

(چهار) بنابر (سه)، $AA^{-1} = I_n$ ایجاب می‌کند که $|A||A^{-1}| = |AA^{-1}| = |I_n| = 1$. از اینرو، $|A|$ در R یکه است و $|A|^{-1} = |A^{-1}|$.

(پنج) به همین نحو، $B = PAP^{-1}$ ایجاب می‌کند که $|B| = |P||A||P|^{-1} = |A|$، زیرا R تعویضپذیر است.

(شش) فرض کنیم $A = (a_{ij})$. هرگاه $i_1, \ldots, i_n$ اعداد صحیح $1, 2, \ldots, n$ به‌ترتیبی خاص باشند، آنگاه، چون R تعویضپذیراست، هر حاصلضرب $a_{i_1 1} a_{i_2 2} \cdots a_{i_n n}$ را می‌توان به صورت $a_{1 j_1} a_{2 j_2} \cdots a_{n j_n}$ نوشت. هرگاه σ جایگشتی باشد که $\sigma(k) = i_k$، آنگاه σ^{-1} جایگشتی است که $\sigma^{-1}(k) = j_k$. به‌علاوه، به‌آسانی معلوم می‌شودکه به‌ازای هر $\sigma \in S_n$، $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$. فرض کنیم $A^t = (b_{ij})$. چون S_n گروه است،

$$|A^t| = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) b_{1\sigma 1} \cdots b_{n\sigma n} = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma 11} \cdots a_{\sigma nn}$$
$$= \sum_{\sigma^{-1} \in S_n} (\operatorname{sgn} \sigma^{-1}) a_{1\sigma^{-1}1} \cdots a_{n\sigma^{-1}n} = |A|.$$

(هفت) طبق فرض، یا به‌ازای هر $j < i$، $a_{ij} = 0$ یا به‌ازای هر $j > i$، $a_{ij} = 0$. در هر حالت، نشان دهید هرگاه $\sigma \in S_n$ و $\sigma \neq (1)$، آنگاه $a_{1\sigma 1} \cdots a_{n\sigma n} = 0$، که از آنجا

$$|A| = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma 1} \cdots a_{n\sigma n} = a_{11} a_{22} \cdots a_{nn}.$$

(هشت) فرض کنیم $X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n$ سطرهای A باشند. هرگاه B دارای سطرهای $X_1, \ldots, X_j, \ldots, X_i, \ldots, X_n$ باشد، آنگاه، چون d متقارن اریب است، طبق قضیهٔ ۲۰۳،

$$\begin{aligned}|B| &= d(X_1, \ldots, X_j, \ldots, X_i, \ldots, X_n)\\ &= -d(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n) = -|A|.\end{aligned}$$

به همین نحو، هرگاه B دارای سطرهای $X_1, \ldots, X_i, \ldots, rX_i + X_j, \ldots, X_n$ باشد، آنگاه، چون d چندخطی و متناوب است،

$$\begin{aligned}|B| &= d(X_1, \ldots, X_i, \ldots, rX_i + X_j, \ldots, X_n)\\ &= rd(X_1, \ldots, X_i, \ldots, X_i, \ldots, X_n) + d(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)\\ &= r0 + |A| = |A|.\end{aligned}$$

حکم دیگر به همین نحو ثابت می‌شود؛ از قسمت (پنج) برای احکام نظیر در مورد ستونها استفاده کنید.

هرگاه R میدان باشد، آنگاه آخرین قسمت قضیهٔ ۵۰۳ روشی برای محاسبهٔ $|A|$ به دست می‌دهد. با استفاده از اعمال سطری و ستونی مقدماتی، A را به ماتریس قطری $B = (b_{ij})$ تغییر داده، در هر مرحله (به وسیلهٔ (هشت)) اثرات آن را بر $|A|$ نظاره می‌کنیم. بنابر قسمت (هشت)، به‌ازای یک $0 \neq r \in R$، $|B| = r|A|$. از اینرو، طبق (هفت)، $r|A| = b_{11}b_{22}\cdots b_{nn}$ و

$$|A| = r^{-1}b_{11}\cdots b_{nn}.$$

به‌طورکلی، دترمینان ماتریس $n \times n$ ، A روی یک حلقهٔ تعویضپذیر و یکدار را می‌توان به‌صورت زیر محاسبه کرد. به‌ازای هر (i,j) ، ماتریس A_{ij} ، $(n-1) \times (n-1)$ است که از حذف سطر i و ستون j از A به دست می‌آید. در این صورت، $|A_{ij}| \in R$ **مینور** $A = (a_{ij})$ در موضع (i,j) است و $(-1)^{i+j}|A_{ij}| \in R$ **همعامل** a_{ij} نام دارد.

حکم ۶۰۳. *هرگاه A یک ماتریس n × n روی حلقهٔ تعویضپذیر و یکدار R باشد، آنگاه به‌ازای هر* $i = 1,2,\ldots,n$ ،

$$|A| = \sum_{j=1}^{n} (-1)^{i+j}a_{ij}|A_{ij}|$$

و ، به‌ازای هر $j = 1,2,\ldots,n$ ،

$$|A| = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}|.$$

فرمول اول [دوم] برای $|A|$ بسط $|A|$ نسبت به سطر i [ستون j] نام دارد .

برهان ۶.۳ . فرض کنیم j ثابت باشدو حکم دوم را اثبات می‌کنیم . بنابر قضیهٔ ۳.۳ و تعریف ۴.۳ ، کافی است نشان دهیم که نگاشت $\phi : \mathrm{Mat}_n R \to R$ داده شده با $A = (a_{ij}) \mapsto \sum_{i=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}|$ یک‌فرم R ــ چندخطی متناوب است به‌طوری‌که $\phi(I_n) = 1_R$.

فرض کنیم $X_1, \ldots, X_n$ سطرهای A باشند . هرگاه $X_k = X_t$ که $1 \le k < t \le n$ ، آنگاه، به‌ازای $i \neq k,t$ ، $|A_{ij}| = 0$ ، زیرا دترمینان یک ماتریس با دو سطر یکسان است . چون A_{kj} را می‌توان از A_{tj} با تعویض متوالی سطر t با سطرهای $t-1, \ldots, k+1$ به دست آورد ، طبق قضیهٔ ۵.۳ ، $|A_{kj}| = (-1)^{t-k-1} |A_{tj}|$. لذا ،

$$\phi(A) = (-1)^{k+j} |A_{kj}| + (-1)^{t+j} |A_{tj}| = (-1)^{k+j+t-k-1} |A_{tj}| + (-1)^{t+j} |A_{tj}| = 0.$$

بنابراین ، ϕ متناوب است . اگربه‌ازای k ای ، $X_k = rY_k + sW_k$ ، فرض می‌کنیم $B = (b_{ij})$ و $C = (c_{ij})$ ماتریسهایی به ترتیب با سطرهای $X_1, \ldots, X_{n-1}, Y_k, X_{k+1}, \ldots, X_n$ و $X_1, \ldots, X_{k-1}, W_k, X_{k+1}, \ldots, X_n$ باشند . برای اثبات R ــ چندخطی بودن ϕ ، کافی است نشان دهیم که $|A_{kj}| = |B_{kj}| = |C_{kj}|$ ، آنگاه $i = k$. هرگاه $\phi(A) = r\phi(B) + s\phi(C)$ ، که از آنجا $a_{kj}|A_{kj}| = (rb_{kj} + sc_{kj})|A_{kj}| = rb_{kj}|B_{kj}| + sc_{kj}|C_{kj}|$. هرگاه $i \neq k$ ، آنگاه ، چون $|A_{ij}|$ تابعی چندخطی از سطرهای A_{ij} بوده و به‌ازای $i \neq k$ ، $a_{ij} = b_{ij} = c_{ij}$ ، داریم

$$a_{ij}|A_{ij}| = a_{ij}(r|B_{ij}| + s|C_{ij}|) = rb_{ij}|B_{ij}| + sc_{ij}|C_{ij}|.$$

پس نتیجه می‌شود که $\phi(A) = r\phi(B) + s\phi(C)$ ؛ از اینرو ، ϕ ، R ــ چندخطی است . واضح است که $\phi(I_n) = 1_R$. بنابراین ، ϕ تابع دترمینان می‌باشد . حکم اول قضیه به‌آسانی با استفاده از ترانهاده‌ها به دست می‌آید .

حکم ۷.۳ . هرگاه $A = (a_{ij})$ یک ماتریس $n \times n$ روی حلقهٔ تعویضپذیر و یکدار R بوده و $A^a = (b_{ij})$ ماتریس $n \times n$ باشد که $b_{ij} = (-1)^{i+j} |A_{ji}|$ ، آنگاه $AA^a = |A| I_n = A^a A$.

به علاوه، A در $Mat_n R$ معکوسپذیر است اگر و فقط اگر $|A|$ در R یکه باشد، که در این حالت $A^{-1} = |A|^{-1}A^a$.

ماتریس A^a الحاق کلاسیک A نام دارد. توجه کنیدکه هرگاه R میدان باشد، $|A|$ یکه است اگر و فقط اگر $|A| \neq 0$.

برهان ۷.۳. درایهٔ (i,j) ی AA^a عبارت است از $c_{ij} = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} |A_{jk}|$. هرگاه $i = j$، آنگاه، بنابر حکم ۶.۳، $c_{ii} = |A|$. اگر $i \neq j$ (مثلا "، $i < j$) و A دارای سطرهای $X_1, \ldots, X_n$ باشد، $B = (b_{ij})$ را ماتریسی با سطرهای

$$X_1, \ldots, X_i, \ldots, X_{j-1}, X_i, X_{j+1}, \ldots, X_n$$

می‌انگاریم. در این صورت، به‌ازای هر k، $b_{ik} = a_{ik} = b_{jk}$ و $|A_{jk}| = |B_{jk}|$؛ بخصوص، $|B| = 0$، زیرا دترمینان یک فرم متناوب است. از اینرو،

$$c_{ij} = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} |A_{jk}| = \sum_{k=1}^{n} (-1)^{i+k} b_{jk} |B_{jk}| = |B| = 0.$$

بنابراین، $c_{ij} = \delta_{ij}|A|$ (دلتای کرونکر) و $AA^a = |A| I_n$. بخصوص، آخرین حکم با A^t به‌جای A برقرار است: $A^t(A^t)^a = |A^t| I_n$. چون $(A^a)^t = (A^t)^a$، داریم

$$|A| I_n = |A^t| I_n = A^t(A^t)^a = A^t(A^a)^t = (A^a A)^t$$

که از آنجا $A^a A = (|A| I_n)^t = |A| I_n$. لذا، اگر $|A|$ یک یکه در R باشد، $|A|^{-1}A^a \in \mathrm{Mat}_n R$ و واضح است که $(|A|^{-1}A^a)A = I_n = A(|A|^{-1}A^a)$. ازاینرو، A معکوسپذیر با معکوس (لزوما " منحصر به فرد) $A^{-1} = |A|^{-1}A^a$ است. به‌عکس، هرگاه A معکوسپذیر باشد، آنگاه، بنابر قضیهٔ ۵.۳، $|A|$ یکه می‌باشد.

نتیجهٔ ۸.۳ (قاعدهٔ کرامر[1]). فرض کنیم $A = (a_{ij})$ ماتریس ضرایب دستگاه n معادلهٔ خطی n مجهولی

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

1. Cramer

روی میدان K *باشد . هرگاه* $|A| \neq 0$ *، آنگاه دستگاه دارای جواب منحصر به فردی است که با*

$$x_j = |A|^{-1}\left(\sum_{i=1}^{n} (-1)^{i+j} b_i |A_{ij}|\right) \qquad j = 1,2,\ldots,n$$

داده می‌شود .

برهان . واضح است که دستگاه‌جواب‌دارداگر و فقط‌اگر معادلهٔ ماتریسی $AX = B$ جواب داشته‌باشد ،که درآن X و B بردارهای‌ستونی $B = (b_1 \cdots b_n)^t$ ، $X = (x_1 \cdots x_n)^t$ می‌باشند . چون $|A| \neq 0$ ، طبق‌حکم ۷.۳ ، A معکوسپذیر است ، و $X = A^{-1}B$ جواب می‌باشد . این جواب منحصر به فرد است ، زیرا $AY = B$ ایجاب می‌کند که $Y = A^{-1}B$. برای به دست آوردن فرمولی جهت x_j ، با استفاده از معادلهٔ

$$X = A^{-1}B = (|A|^{-1}A^a)B = |A|^{-1}(A^aB)$$

حساب می‌کنیم .

تمرینات

تذکر . درایه‌های تمام ماتریسها در حلقهٔ تعویضپذیر و یکدار R قرار دارند مگر خلافش گفته شود .

۱ . هرگاه بـه‌ازای جمیـع $r \in R$ های نـاصفر $r + r \neq 0$ ، آنگاه ثابت کنید یک فرم n خطی $B^n \to R$ متناوب است اگر و فقط‌اگر متقارن اریب باشد . اگر $\text{char } R = 2$ چه وضعی داریم ؟

۲ . (آ) هرگاه $m > n$ ، آنگاه هـر فرم R ــ چندخطی متناوب بر $(R^n)^m$ صفر است .
(ب) هرگاه $m < n$ ، آنگاه‌فرم R ــ چندخطی‌متناوب‌ناصفربر $(R^n)^m$ وجود دارد .

۳ . با استفاده‌ازتمرین۲ ، مستقیما " ثابت کنید هرگاه یک یکریختی R ــ مدولها مانند $R^m \cong R^n$ موجود باشد ، آنگاه $m = n$.

۴ . هرگاه $A \in \text{Mat}_n R$ ، آنگاه $|A^a| = |A|^{n-1}$ و $(A^a)^a = |A|^{n-2}A$.

۵ . هرگاه R میدان بـوده و $A,B \in \text{Mat}_n R$ معکوسپذیر باشد ، آنگاه ماتریس $A + rB$ به جز تعدادی متناهی $r \in R$ ، همواره معکوسپذیر است .

۶ . فرض کنیـد A یک ماتـریس $n \times n$ روی یـک میدان باشد . بدون استفاده از حکم

۷.۳ ثابت کنید A معکوسپذیر است اگر و فقط اگر $|A| \neq 0$. [**راهنمایی .** قضایای ۶.۲ و ۵.۳ (هشت) و حکم ۱۲.۲ .]

۷ . فرض کنید F یک R ــ مدول آزاد با پایهٔ $U = \{u_1, \ldots, u_n\}$ باشد . هرگاه $\phi : F \to F$ یک درونریختی R ــ مدولها با ماتریس A نسبت به U باشد ، آنگاه **دترمینان درونریختی** ϕ با $|A| \in R$ تعریف شده و با $|\phi|$ نموده می‌شود .

(آ) $|\phi|$ از انتخاب U مستقل است .

(ب) $|\phi|$ عنصر منحصر به فردی از R است به‌طوری‌که به‌ازای هر فرم R-چندخطی متناوب بر F^n و تمام $b_i \in F$ ها ، $f(\phi(b_1), \phi(b_2), \ldots, \phi(b_n)) = |\phi| f(b_1, \ldots, b_n)$.

۸ . فرض کنید $(b_1, \ldots, b_n)$ جواب دستگاه معادلات خطی همگن

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

بوده و $A = (a_{ij})$ ماتریس $n \times n$ ضرایب باشد . در این صورت ، به‌ازای هر i ، $|A|b_i = 0$. [**راهنمایی .** هرگاه B_i ماتریس قطری $n \times n$ با درایه‌های قطری $|AB_i| = |A|b_i$ باشد ، آنگاه $1_R, \ldots, 1_R, b_i, 1_R, \ldots, 1_R$. برای اثبات $|AB_i| = 0$ ، b_i برابر ستون j از AB_i را به ستون i ، به‌ازای هر $j \neq i$ ، بیفزایید . ماتریس حاصل دارای دترمینان $|AB_i|$ بوده و در آن درایهٔ (k,i) ی $a_{k1}b_1 + a_{k2}b_2 + \cdots + a_{kn}b_n = 0$ ، به‌ازای $k = 1, 2, \ldots, n$ ، می‌باشد .]

۴ تجزیهٔ یک تبدیل خطی و تشابه

ساختار فضای برداری با بعد متناهی E روی میدان K نسبت به تبدیل خطی $E \to E$ بررسی شد . تبدیل خطی تجزیه‌ای از E به صورت مجموع مستقیمی از زیرفضاها را القا کرده و به هر تجزیهٔ E از این نوع مجموعه‌ای از پایاهای چندجمله‌ای در $K[x]$ را مربوط می‌سازد (قضیهٔ ۲.۴) . با این مجموعه‌ها از پایاهای چندجمله‌ای می‌توان پایه‌های مختلفی از E اختیار کرد که ماتریس تبدیل خطی داده شده نسبت به هر یک از آنها از نوع خاصی باشد (قضیهٔ ۶.۴) . این امر ما را به شکلهای کانونی مختلفی برای رابطهٔ تشابه در $Mat_n K$ می‌رساند (نتیجهٔ ۷.۴) .

تذکر. نتایج ایـن بخش قویا" به قضایای ساختاری مدولهای با تولید متناهی روی یک دامنهٔ ایده‌آل اصلی بستگی دارند (بخش IV ۶۰) .

فرض کنیـم K یک‌میدان بوده و $\phi: E \to E$ تبدیلی خطی از K ــ فضای برداری n بعدی E باشد . ابتدا چند مطلب در باب ساختار $\mathrm{Hom}_K(E,E)$ و $\mathrm{Mat}_n K$ یادآور می‌شویم. $\mathrm{Hom}_K(E,E)$ تنها یک حلقهٔ یکدار نیست (تمرین IV ۷۰۱۰) ، بلکه فضایی برداری روی K بـه‌ازای $(k\psi)(u) = k\psi(u)$ نیز می‌باشد ($k \in K, u \in E, \psi \in \mathrm{Hom}_K(E,E)$ ؛ر.ک. تبصرهٔ بعد از قضیهٔ IV ۸۰۴۰) . بنابراین ، هرگاه $f = \sum k_i x^i$ یک چندجمله‌ای در $K[x]$ باشد ، آنگاه $f(\phi) = \sum k_i \phi^i$ یک عنصـر تعریف شده از $\mathrm{Hom}_K(E,E)$ است (که در آن ، طبق معمول ، $\phi^0 = 1_E$) . به همین نحو ، حلقهٔ $\mathrm{Mat}_n K$ نیز یک فضـای بـرداری روی K است . هرگاه $A \in \mathrm{Mat}_n K$ ، آنگاه $f(A) = \sum k_i A^i$ یک ماتـریس $n \times n$ تعریف شده روی K (بـه‌ازای $A^0 = I_n$) می‌باشد .

قضیهٔ ۱۰۴ . *فرض کنیم E یک فضای برداری n بعدی روی میدان K ، $\phi: E \to E$ یک تبدیل خطی ، و A یک ماتریس $n \times n$ روی K باشد .*

(یک) یک چندجمله‌ای تکین منحصر به فرد از درجهٔ مثبت مانند $q_\phi \in K[x]$ وجود دارد به‌طوری‌که $q_\phi(\phi) = 0$ و ، به‌ازای هر $f \in K[x]$ که $f(\phi) = 0$ ، $q_\phi \mid f$.

(دو) یک چندجمله‌ای تکین منحصر به فرد از درجهٔ مثبت مانند $q_A \in K[x]$ وجود دارد به‌طوری‌که $q_A(A) = 0$ و ، به‌ازای هر $f \in K[x]$ که $f(A) = 0$ ، $q_A \mid f$.

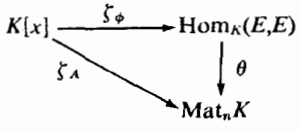
(سه) هرگاه A ماتریس ϕ نسبت به پایه‌ای از E باشد ، آنگاه $q_A = q_\phi$.

برهان. (یک) بنابرقضیهٔ III ۵۰۵۰ ، یک‌همریختی (ناصفر) منحصر به فرد از حلقه‌ها مانند $\zeta: K[x] \to \mathrm{Hom}_K(E,E)$ ، $\zeta = \zeta_\phi$ وجود دارد به‌طوری‌که $x \mapsto \phi$ و ، به‌ازای هر $k \in K$ ، $k \mapsto k1_E$. درنتیجه ، هرگاه $f \in K[x]$ ، آنگاه $\zeta(f) = f(\phi)$. به آسانی معلوم می‌شودکه ζ یک تبدیل خطی از K ــ فضاهای بـرداری اسـت . چون $\dim_K E$ متناهی است ، بنابر قضایای IV ۱۰۲۰ ، IV ۴۰۲۰ ، IV ۷۰۴۰ ، و IV ۹۰۴۰ ، $\mathrm{Hom}_K(E,E)$ روی K با بعد متناهی است . لذا ، $\mathrm{Im}\,\zeta$ لزوما" روی K با بعد متناهی می‌باشد . چون $K[x]$ روی K

با بعد نامتناهی است، بنابرنتیجهٔ IV ۱۴.۲۰ ، باید داشته باشیم $\operatorname{Ker}\zeta \neq 0$. چون $K[x]$ یک دامنهٔ ایده‌آل اصلی است که یکه‌هایش دقیقاً" عناصر ناصفر K اند (نتیجهٔ III ۴.۶۰) ، به‌ازای یک‌چندجمله‌ای‌تکین مانند $q \in K[x]$ ، $\operatorname{Ker}\zeta = (q)$. چون ζ نگاشت صفر نیست ، $(q) \neq K[x]$ ، که از آنجا $\deg q \geq 1$. هرگاه $\operatorname{Ker}\zeta = (q_1)$ که $q_1 \in K[x]$ تکین است ، آنگاه ، بنابر قضیهٔ III ۲.۳۰ ، $q \mid q_1$ و $q_1 \mid q$ ، که از آنجا $q = q_1$ ، زیرا هر دو تکین می‌باشند . لذا ، $q_\phi = q$ خواص ذکر شده را دارا می‌باشد .

(دو) برهان همان‌برهان (یک) است‌که‌درآن A به‌جای ϕ و $\mathbf{Mat}_n K$ به‌جای $\mathbf{Hom}_K(E,E)$ نشسته است . $q_A \in K[x]$ تنها چندجمله‌ای تکین است که $(q_A) = \operatorname{Ker}\zeta_A$ ، که در آن $\zeta_A : K[x] \to \mathbf{Mat}_n K$ همریختی منحصر به فردی از حلقه‌ها است که با $f \mapsto f(A)$ داده می‌شود .

(سه) فرض‌کنیم A ماتریس ϕ نسبت به پایهٔ U از E بوده و $\theta : \mathbf{Hom}_K(E,E) \cong \mathbf{Mat}_n R$ یکریختی قضیهٔ ۲.۱ باشد ؛ درنتیجه ، $\theta(\phi) = A$. بنابر قضیهٔ III ۵.۵۰ ، نمودار



تعویضپذیر است ، زیرا $\theta\zeta_\phi(x) = \theta(\phi) = A = \zeta_A(x)$ و ، به‌ازای هر $k \in K$ ،

$$\theta\zeta_\phi(k) = \theta(k1_E) = kI_n = \zeta_A(k) .$$

چون θ یکریختی است ، $(q_\phi) = \operatorname{Ker}\zeta_\phi = \operatorname{Ker}\theta\zeta_\phi = \operatorname{Ker}\zeta_A = (q_A)$. بنابراین ، $q_\phi \mid q_A$ و $q_A \mid q_\phi$ ، که از آنجا $q_\phi = q_A$ ، زیرا هر دو تکین هستند .

هرگاه K ، E ، و ϕ همانند درقضیهٔ ۱.۴ باشند ، آنگاه چندجمله‌ای q_ϕ [q_A] **چندجمله‌ای مینیمال** تبدیل خطی ϕ [ماتریس A] نام دارد. درحالت کلی ، q_ϕ تحویل‌ناپذیر نیست . ازنتیجهٔ ۷.۱ وقضیهٔ ۱.۴ (سه) فوراً" نتیجه می‌شود که ماتریسهای متشابه چندجمله‌ای مینیمال یکسان دارند .

فرض‌کنیم K ، E ، و ϕ همانند فوق باشند . در این صورت ، ϕ یک ساختار $K[x]$ ــ مدول (چپ) بر E به صورت زیر القا می‌کند . هرگاه $f \in K[x]$ و $u \in E$ ، آنگاه $f(\phi) \in \mathbf{Hom}_K(E,E)$ و fu به‌وسیلهٔ $fu = f(\phi)(u)$ تعریف شده است . گوییم K ــ زیرفضای

F از E تحت ϕ پایا (یا ϕ ــ پایا) است اگر $\phi(F) \subset F$. واضح است که F یک ϕ ــ پایای K ــ زیرفضا است اگر و فقط اگر F یک $K[x]$ـ زیرمدول E باشد. بخصوص، به‌ازای هر $v \in E$، زیرفضای $E(\phi,v)$ پیموده شده به وسیلهٔ مجموعهٔ $\{\phi^i(v) \mid i \geq 0\}$، ϕ ــ پایا است. به آسانی معلوم می‌شود که $E(\phi,v)$ درست $K[x]$ ــ زیرمدول دوری $K[x]v$ است که به وسیلهٔ v تولید می‌شود. $E(\phi,v)$ یک (زیر) فضای ϕ ــ دوری نامیده می‌شود.

قضیهٔ ۲۰۴. فرض کنیم $\phi : E \to E$ یک تبدیل خطی از فضای برداری n بعدی E روی میدان K باشد.

(یک) چندجمله‌ایهای تکین $q_1, q_2, \ldots, q_t \in K[x]$ از درجهٔ مثبت و زیرفضاهای ϕ ــ دوری $E_1, \ldots, E_t$ از E وجود دارند به‌طوری‌که $E = E_1 \oplus E_2 \oplus \cdots \oplus E_t$ و $q_1 \mid q_2 \mid \cdots \mid q_t$. به‌علاوه، $(q_1, \ldots, q_t)$ با q_i چندجمله‌ای مینیمال $\phi \mid E_i : E_i \to E_i$ می‌باشد. دنبالهٔ q_i و ϕ به‌طور منحصر به‌فرد معین می‌شود و q_t چندجمله‌ای مینیمال ϕ است.

(دو) چندجمله‌ایهای تحویل‌ناپذیر تکین $p_1, \ldots, p_s \in K[x]$ و زیرفضاهای ϕ ــ دوری $E_{11}, \ldots, E_{1k_1}, E_{21}, \ldots, E_{2k_2}, E_{31}, \ldots, E_{sk_s}$ از E وجود دارند به‌طوری‌که $E = \sum_{i=1}^{s} \sum_{j=1}^{k_i} E_{ij}$ و، به‌ازای هر i، یک دنبالهٔ ناصعودی از اعداد صحیح مانند $m_{i1} \geq m_{i2} \geq \cdots \geq m_{ik_i} \geq 0$ وجود دارند به‌طوری‌که $p_i^{m_{ij}}$ چندجمله‌ای مینیمال $\phi \mid E_{ij} : E_{ij} \to E_{ij}$ می‌باشد. خانوادهٔ $\{p_i^{m_{ij}} \mid 1 \leq i \leq s; 1 \leq j \leq k_i\}$ از چندجمله‌ایها به‌طور منحصر به فرد به وسیلهٔ E و ϕ معین می‌شود و $p_1^{m_{11}} p_2^{m_{21}} \cdots p_s^{m_{s1}}$ چندجمله‌ای مینیمال ϕ می‌باشد.

چندجمله‌ایهای $q_1, \ldots, q_t$ مذکور در قسمت (یک) قضیه عاملهای پایای تبدیل خطی ϕ نام دارند. چندجمله‌ایهای $p_i^{m_{ij}}$ با توان اول آمده در قسمت (دو) مقسوم‌علیه‌های مقدماتی ϕ نامیده می‌شوند.

طرح برهان ۲۰۴. (یک) همانطورکه در بالا ذکر شد، E یک مدول چپ روی دامنهٔ ایده‌آل اصلی $K[x]$ است که $(f \in K[x], u \in E)$ $fu = f(\phi)(u)$. چون E روی K با بعد متناهی بوده و $K \subset K[x]$، E لزوماً یک $K[x]$ ــ مدول ناصفر با تولید متناهی است. هرگاه q_ϕ چندجمله‌ای مینیمال ϕ باشد، آنگاه $q_\phi \neq 0$ و $q_\phi E = 0$، که از آنجا E یک

$K[x]$ ــ مدول تـابی خـواهد بود. بنابر قضیهٔ IV ۱۲.۶۰ (یک)، E مجموع مستقیم داخلی $E = E_1 \oplus \cdots \oplus E_t$ است، کـه در آن هر E_i یک $K[x]$ ــ مدول دوری ناصفر از مرتبهٔ q_i $(q_i \in K[x])$ بوده و $q_1 \mid q_2 \mid \cdots \mid q_t$. بنابر تبصره‌های پیش از قضیه، هر E_i یک زیرفضای ϕ ــ دوری است. چون E_i از مرتبهٔ q_i است، بنابر قضیهٔ IV ۴.۶۰ و مثال بعد از آن، یک یکریختی $K[x]$ ــ مدولها مانند $E_i \cong K[x]/(q_i)$ وجود دارد. چون $E_i \neq 0$ و هر ایده‌آل ناصفر در $K[x]$ مولد تکین منحصر به فرد دارد (قضیهٔ III ۲.۳۰ و نتیجهٔ III ۴.۶۰)، می‌توان فرض کرد هر q_i تکین و از درجهٔ مثبت است. حکم یکتایی قضیهٔ IV ۱۲.۶۰ (یک) و این امر که $q_1 \mid q_2 \mid \cdots \mid q_t$ ایجاب می‌کنند که $q_1, \ldots, q_t$ به وسیلهٔ $K[x]$ ــ مدول E (یعنی، بـه وسیلهٔ E و ϕ) به‌طور منحصر به فرد معین شـوند. با استفاده از ساختار $K[x]$ ــ مدول E_i و اینکه E_i دوری از مرتبهٔ q_i است، تحقیق کنید که چندجمله‌ای مینیمال E_i $\mid \phi$ مساوی q_i است. بالاخره، $q_t E = q_t(\phi)E_1 \oplus \cdots \oplus q_t(\phi)E_t = 0$، کـه از آنجـا $(q_\phi) \subset (q_t)$. چون $q_\phi E = 0$، داریم $q_\phi E_t = 0$، که از آنجا $(q_t) \subset (q_\phi)$. درنتیجه، $q_t = q_\phi$، زیرا هردو تکین بوده و $(q_\phi) = (q_t)$. قسمت دوم قضیه به همین نحو، با تجزیهٔ E به مجموع مستقیم $K[x]$ ــ زیرمدولهای دوری که مرتبه‌هایشان توانی از اعداد اولند، ثابت خواهد شد (قضیهٔ IV ۱۲.۶۰ (دو)).

تبصره. هرگاه $\phi = 0$، آنگاه برهان قضیهٔ ۲.۴ نشان می‌دهد که چندجمله‌ای مینیمال ϕ مساوی x بوده و عـوامـل پـایا [مقسـوم علیه‌هـای مقـدماتـی] آن عبـارتند از $q_1 = x, q_2 = x, \ldots, q_n = x$. (تمرین ۲).

برهان قضیهٔ ۲.۴ نشان می‌دهد که عوامل پایا و مقسوم علیه‌های مقدماتی تبدیل خطی $\phi : E \to E$ چیزی جز عوامل پایا و مقسوم علیه‌های مقدماتی $K[x]$ ــ مدول E نیستند. درنتیجه، همانند در برهان قضیهٔ IV ۱۲.۶۰، می‌توان مقسوم علیه‌های مقدماتی را از عوامل پایا و بالعکس به دست آورد (همچنین، ر.ک. صفحات ۱۲۴ تا ۱۲۵). در حکم ۹.۴ زیر، تکنیکی برای محاسبهٔ عوامل پایای یک تبدیل خطی مشخص مطرح خواهد شد.

مثال. فرض کنیـم $K = \mathbf{Q}$ و $\dim_K E = 15$ و عوامـل پـایـای ϕ عبـارت باشند از $q_1 = x^4 - x^2 - 2$، $q_2 = x^5 - x^3 - 2x$، و $q_3 = x^6 - x^4 - 2x^2$. پس

$$q_1 = (x^2 - 2)(x^2 + 1),$$

$q_2 = xq_1$ ، و $q_3 = xq_2$ ، که از آنجا مقسوم‌علیه‌های مقدماتی ϕ عبارت خواهند بود از $x^2 - 2, x^2 + 1, x, x^2 - 2, x^2 + 1, x^2, x^2 - 2, x^2 + 1$ و نیز ص۱۲۴. بـه عکس، هرگاه مقسوم‌علیه‌های مقدماتی تبدیل خطی ψ عبارت باشند از $x - 1$ ، $x - 1$ ، $x - 2$ ، $x - 3$ ، $(x - 2)^2$ ، $x^2 + 1$ ، $x^2 + 1$ ، $x^2 + 1$ و $(x - 1)^3$ ، آنگاه عوامل پایا مساویند با $q_1 = (x - 1)(x^2 + 1)$، $q_2 = (x - 1)(x - 2)(x^2 + 1)$، و $q_3 = (x - 3)(x - 2)^2(x^2 + 1)(x - 1)^3$.

به خـاطر قضیهٔ ۲۰۴ ، گام بعدی تحلیل باید بررسی فضاهای ϕ ــ دوری باشد .

قضیهٔ ۳۰۴ . *فرض کنیم $\phi : E \to E$ تبدیلی خطـی از فضای برداری با بعد متناهی E روی میدان K باشد . E یک فضـای ϕ ــ دوری اسـت و ϕ دارای چندجمله‌ای مینیمال $q = x^r + a_{r-1}x^{r-1} + \cdots + a_0 \in K[x]$ است اگـر و فقط اگر $dim_K E = r$ و E پایهٔ مرتب V را داشته باشد که ماتریس ϕ نسبت به آن مساوی*

$$A = \begin{pmatrix} 0 & 1_K & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1_K & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1_K & 0 & \cdots & 0 & 0 \\ \cdot & & & & & & & \cdot \\ \cdot & & & & & & & \cdot \\ \cdot & & & & & & & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1_K \\ -a_0 & -a_1 & -a_2 & -a_3 & -a_4 & \cdots & -a_{r-2} & -a_{r-1} \end{pmatrix}$$

باشد . دراین حالت ، به‌ازای $v \in E$ ای ، $V = \{v, \phi(v), \phi^2(v), \ldots, \phi^{r-1}(v)\}$.

ماتریس A *ماتریس همراه* چندجمله‌ای تکین $q \in K[x]$ نام دارد .[1] توجه‌کنید که هرگاه $q = x + a_0$ ، آنگاه $A = (-a_0)$.

---

۱. *هرگاه E را یک K ــ فضای‌برداری راست گرفته‌وماتریسهای نگاشتها بر این طبق (مثل ص ۵۲۱) ساخته شوند ، آنگاه ، برای برقراری قضیه ، ماتریس همراه q باید مساوی A^t تعریف گردد .*

برهان ۳.۴. ($\Leftarrow$) هرگاه E ، ϕ ــ دوری باشد ، آنگاه تبصره‌های پیش از قضیهٔ ۲.۴ نشان می‌دهند که ، به‌ازای $v \in E$ ای ، E ، $K[x]$ ــ مدول دوری $K[x]v$ است ، که در آن ساختار $K[x]$ ــ مدول به‌وسیلهٔ ϕ القاشده است . هرگاه $k_0v + k_1\phi(v) + \cdots + k_{r-1}\phi^{r-1}(v) = 0$ $(k_i \in K)$ ، آنگاه $f = k_0 + k_1x + \cdots + k_{r-1}x^{r-1}$ یک چندجمله‌ای است به‌طوری که $f(\phi)(v) = 0$ که از آنجا ، بر $E = K[x]v$ ، $f(\phi) = 0$. چون ، بنابر قضیهٔ ۱.۴ (یک) ، $\deg f \leq r - 1 < \deg q$ و $q \mid f$ ، باید به‌ازای هر i داشته باشیم $k_i = 0$. بنابراین ، $\{v, \phi(v), \ldots, \phi^{r-1}(v)\}$ مستقل‌خطی می‌باشد . هرگاه $fv = f(\phi)(v)$ $(f \in K[x])$ عنصردلخواهی از $E = K[x]v$ باشد ، آنگاه ، بنابرالگوریتم تقسیم ، $f = qh + s$ ، که در آن $s = \sum_{i=1}^{t} k_ix^i$ از درجهٔ t بوده و $t < \deg q$. درنتیجه ، $f(\phi) = q(\phi)h(\phi) + s(\phi) = 0 + s(\phi) = s(\phi)$ و $fv = f(\phi)(v) = s(\phi)(v) = k_0 + k_1\phi(v) + \cdots + k_t\phi^t(v)$ ، که در آن $t \leq s - 1$. بنابراین ، $\{v, \phi(v), \ldots, \phi^{r-1}(v)\}$ E را می‌پیماید ؛ و درنتیجه ، یک پایه می‌باشد . چون $q(\phi) = 0$ ، داریم

$$\phi(\phi^{r-1}(v)) = \phi^r(v) = -a_0v - a_1\phi(v) - \cdots - a_{r-1}\phi^{r-1}(v) .$$

بی‌درنگ نتیجه می‌شود که ماتریس ϕ نسبت به $\{v, \phi(v), \ldots, \phi^{r-1}(v)\}$ ماتریس‌همراه q می‌باشد .

($\Rightarrow$) هرگاه A ماتریس ϕ نسبت‌به‌پایهٔ $\{v = v_1, v_2, \ldots, v_r\}$ باشد ، آنگاه محاسبه‌ای ساده نشان می‌دهد که ، به‌ازای $i = 2, \ldots, r$ ، $v_i = \phi^{i-1}(v)$ و

$$\phi^r(v) = \phi(v_r) = -a_0v - a_1\phi(v) - \cdots - a_{r-1}\phi^{r-1}(v) .$$

درنتیجه ، E فضای ϕ ــ دوری تولید شده به وسیلهٔ v است و $E = K[x]v$. چون $q(\phi)(v) = 0$ ، بر E داریم $q(\phi) = 0$. چون $\{v, \phi(v), \ldots, \phi^{r-1}(v)\}$ مستقل خطی است ، نمی‌تواند $f \in K[x]$ ی ناصفر از درجهٔ کمتر از r وجود داشته باشد که $f(\phi) = 0$. حال‌ازالگوریتم‌تقسیم نتیجه می‌شود که q چندجمله‌ای مینیمال ϕ است .

نتیجهٔ ۴.۴ . *فرض کنیم $\psi : E \to E$ تبدیلی خطی از فضای برداری با بعد متناهی E روی‌میدان K باشد . E یک‌فضای ψ ــ دوری و ψ با چندجمله‌ای‌مینیمال $q = (x - b)^r$ $(b \in K)$ است اگر و فقط اگر $\dim_K E = r$ و E پایهٔ مرتبی داشته باشد که ماتریس ψ نسبت به آن*

مساوی

$$B = \begin{pmatrix} b & 1_K & 0 & 0 & \cdots & 0 & 0 \\ 0 & b & 1_K & 0 & \cdots & 0 & 0 \\ 0 & 0 & b & 1_K & \cdots & 0 & 0 \\ \cdot & & & & & & \cdot \\ \cdot & & & & & & \cdot \\ \cdot & & & & & & \cdot \\ 0 & 0 & 0 & 0 & \cdots & b & 1_K \\ 0 & 0 & 0 & 0 & \cdots & 0 & b \end{pmatrix}$$

باشد.

ماتریس $r \times r$ ، B **ماتریس ژردان مقدماتی** مربوط به $(x-b)^r \in K[x]$ نام دارد. توجه کنید که به‌ازای $r = 1$ ، $B = (b)$.

طرح برهان ۴.۴ . فرض کنیم $\phi = \psi - b1_E \in \mathrm{Hom}_K(E,E)$. پس $q = (x-b)^r$ چندجمله‌ای مینیمال ψ است اگر و فقط اگر x^r چندجمله‌ای مینیمال ϕ باشد (مثلا" ، $\phi^r = (\psi - b1_E)^r = q(\psi) = 0$) . E دارای دو ساختار $K[x]$ ــ مدول است که به وسیلهٔ ϕ و ψ القا می‌شوند. به‌ازای هر $f \in K[x]$ و $v \in E$ ، $f(x)v$ در ϕ ــ ساختار همان عنصر $f(x-b)v$ در ψ ــ ساختار است. بنابراین ، E ، ϕ ــ دوری است اگر و فقط اگر E ، ψ ــ دوری باشد. چون $\psi = \phi + b1_E$ ، قضیهٔ ۲.۱ نشان می‌دهد که ماتریس ϕ نسبت به پایهٔ (مرتب) داده شدهٔ E ماتریس‌همراه A از x^r است اگر و فقط اگر ماتریس ψ نسبت به‌همین پایه ماتریس ژردان مقدماتی $B = A + bI_n$ مربوط به $(x-b)^r$ باشد. برای اتمام برهان کافی است قضیهٔ ۳.۴ را بر ϕ اعمال کرده و ، با استفاده از نکاتی که هم‌اکنون ذکر شد ، نتیجه را به احکام مربوط به ψ سرایت دهیم .

برای استفاده‌ازنتایج پیشگفته‌دربه دست آوردن مجموعه‌ای از شکلهای کانونی برای رابطهٔ تشابه بر $\mathrm{Mat}_n K$ ، به لم زیر نیاز خواهیم داشت .

لم ۵.۴ . فرض کنیم $\phi : E \to E$ **تبدیلی‌خطی از فضای برداری** n **بعدی** E **روی میدان** K **باشد. به‌ازای هر** $i = 1, \ldots, t$ ، فرض کنیم M_i **یک ماتریس** $n_i \times n_i$ **روی** K **باشد ،که** $n_1 + n_2 + \cdots + n_t = n$. پس $E = E_1 \oplus E_2 \oplus \cdots \oplus E_t$ ، **که درآن هر** E_i **یک زیرفضای**

ϕ ـ پایای E بوده و، به‌ازای هر i ، M_i ماتریس $\phi \mid E_i$ نسبت به پایهٔ مرتبی از E_i است اگر و فقط اگر ماتریس ϕ نسبت به پایهٔ مرتبی از E مساوی

$$M = \begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_t \end{pmatrix}$$

باشد که در آن قطر اصلی هر M_i بر قطر اصلی M واقع است.

هر ماتریس به شکل M در لم ۵۰۴ مجموع مستقیم از ماتریسهای $M_1, \ldots, M_t$ (به همین ترتیب) نام دارد.

طرح برهان ۵۰۴. ($\Leftarrow$) فرض کنیم V_i ، به‌ازای هر i ، یک پایهٔ مرتب از E_i باشد به‌طوری‌که ماتریس $\phi \mid E_i$ نسبت به V_i مساوی M_i است. چون $E = E_1 \oplus \cdots \oplus E_t$ ، به آسانی نتیجه می‌شود که $V = \bigcup_{i=1}^{t} V_i$ پایه‌ای از E است. تحقیق کنید که M ماتریس ϕ نسبت به V است (که در آن V به نحو روشنی مرتب است). ($\Rightarrow$) به عکس، فرض کنیم $U = \{u_1, \ldots, u_n\}$ پایه‌ای از E بوده و M ماتریس ϕ نسبت به U باشد. همچنین، E_1 زیرفضای E با پایهٔ $\{u_1, \ldots, u_{n_1}\}$ باشدو، به‌ازای $i > 1$ ، E_i زیرفضایی از E با پایهٔ $\{u_{r+1}, \ldots, u_{r+n_i}\}$ باشد، که در آن $r = n_1 + n_2 + \cdots + n_{i-1}$. در این صورت، $E = E_1 \oplus E_2 \oplus \cdots \oplus E_t$ ، که در آن هر E_i ، ϕ ـ پایا بوده و M_i ماتریس $\phi \mid E_i$ نسبت به $\{u_{r+1}, \ldots, u_{r+n_i}\}$ است.

قضیهٔ ۶۰۴. فرض کنیم $\phi : E \to E$ تبدیلی خطی از فضای برداری n بعدی روی میدان K باشد.

(یک) E پایه‌ای دارد که ماتریس ϕ نسبت به آن مجموع مستقیم ماتریسهای همراه عوامل پایای $q_1, \ldots, q_t \in K[x]$ از ϕ است.

(دو) E پایه‌ای دارد که ماتریس ϕ نسبت به آن مجموع مستقیم ماتریسهای همراه مقسوم علیه‌های مقدماتی $p_1^{m_{11}}, \ldots, p_s^{m_{ks}} \in K[x]$ از ϕ است.

(سه) هرگاه چندجمله‌ای مینیمال q از ϕ به‌صورت $q = (x - b_1)^{r_1}(x - b_2)^{r_2} \cdots (x - b_d)^{r_d}$

$(b_i \in K)$ تجزیه شود، که همواره در صورتی که K به‌طور جبری بسته‌باشد چنین است، آنگاه هر مقسوم‌علیه مقدماتی ϕ به شکل $(x - b_i)^j$ $(j \leq r_i)$ است و E پایه‌ای دارد که ماتریس ϕ نسبت به آن مجموع مستقیم ماتریسهای ژردان مقدماتی مربوط به مقسوم‌علیه‌های مقدماتی ϕ می‌باشد.

اثبات، که نتیجه‌ای فوری از نتایج ۲۰۴ تا ۵۰۴ (و یکتایی تجزیه در $K[x]$ برای (سه)) است، به خواننده واگذار می‌شود. نتیجهٔ زیر بی‌درنگ دو (یا سه اگر K به‌طوری جبری‌بسته‌باشد) مجموعه ازشکلهای‌کانونی‌برای‌رابطهٔ تشابه بر $\mathrm{Mat}_n K$ به دست می‌دهد.

نتیجهٔ ۷۰۴. فرض‌کنیم A یک ماتریس $n \times n$ روی میدان K باشد.

(یک) A با ماتریس D متشابه است به‌طوری‌که D مجموع مستقیم ماتریسهای همراه خانواده‌ای منحصر به‌فرد از چندجمله‌ایهای $q_1, \ldots, q_t \in K[x]$ است که $q_1 \mid q_2 \mid \cdots \mid q_t$. ماتریس D به‌طور منحصر به فرد معین می‌شود.

(دو) A با ماتریس M متشابه است به‌طوری‌که M مجموع مستقیم ماتریسهای همراه خانواده‌ای منحصر به فرد از چندجمله‌ایهای با توان اول $p_1^{m_{11}}, \ldots, p_s^{m_{sk_s}} \in K[x]$ است، که در آن هر p_i در $K[x]$ اول (تحویل‌ناپذیر) می‌باشد. M، صرف‌نظر از ترتیب ماتریسهای همراه $p_i^{m_{ij}}$ در امتداد قطر اصلی آن، به‌طور منحصر به فرد معین می‌شود.

(سه) هرگاه K به‌طور جبری بسته باشد، آنگاه A با ماتریس J متشابه است به‌طوری‌که J مجموع مستقیم ماتریسهای ژردان مقدماتی مربوط به خانوادهٔ منحصر به فردی از چندجمله‌ایها به شکل $(b \in K)\ (x - b)^m$ می‌باشد. J، صرف‌نظر از ترتیب ماتریسهای ژردان مقدماتی در امتداد قطر اصلی آن، به‌طور منحصر به فرد معین می‌شود.

برهان در زیر داده می‌شود. گوییم ماتریس D قسمت (یک) به شکل کانونی گویا یا به شکل کانونی گویا از ماتریس A است. به همین نحو، گوییم ماتریس M قسمت (دو) به شکل کانونی گویای اول است و ماتریس J در قسمت (سه) به شکل کانونی ژردان می‌باشد.[1] واژهٔ "گویا" اشاره بدان دارد که تشابه ماتریسها در میدان K رخ می‌دهد نه

---

۱. توجه کنید که بعضی از مولفان شکلهای کانونی گویا و ژردان را به نوع دیگر تعریف می‌کنند.

در توسیع میدان K (ر.ک. تمرین ۷) . چندجمله‌ایهای منحصر به فرد $q_1, \ldots, q_t$ در قسمت (یک) **عوامل پایای ماتریس** A نام دارند . به همین نحو ، چندجمله‌ایهای منحصر به فرد با توان اول $p_i^{m_{ij}}$ در قسمت (دو) **مقسوم‌علیه‌های مقدماتی ماتریس** A نامیده می‌شوند .

طرح برهان ۷.۴ . (دو) فرض کنیم $\phi : K^n \to K^n$ تبدیل خطی با ماتریس A نسبت به پایهٔ متعارف باشد (قضیهٔ ۲.۱) . نتیجهٔ ۷.۱ و قضیهٔ ۶.۴ نشان می‌دهندکه A با ماتریس D متشابه است ؛ که آن مجموع مستقیم ماتریسهای همراه مقسوم‌علیه‌های مقدماتی $p_i^{m_{ij}}$ از ϕ می‌باشد . هرگاه A با D_1 نیز متشابه باشد ، که D_1 مجموع مستقیم ماتریسهای همراه خانواده‌ای از چندجمله‌ایهای $f_1, \ldots, f_b \in K[x]$ با توان اول باشد ، آنگاه D_1 ماتریس ϕ نسبت به‌پایه‌ای‌از K^n است (نتیجهٔ ۷.۱) . بنابر قضیهٔ ۳.۴ و لم ۵.۴ ، $K^n = E_1 \oplus E_2 \oplus \cdots \oplus E_b$ ، که در آن هر E_i یک زیرفضای ϕ ـ دوری بوده و f_i چندجمله‌ای مینیمال $\phi \mid E_i$ است . حکم یکتایی قضیهٔ ۲.۴ ایجاب می‌کندکه چندجمله‌ایهای f_i دقیقاً " مقسوم‌علیه‌های مقدماتی $p_i^{m_{ij}}$ از ϕ اند ؛ درنتیجه تفاوت D با D_1 فقط در ترتیب ماتریسهای همراه $p_i^{m_{ij}}$ ها در امتداد قطر اصلی است . برهان (یک) و (سه) مشابه است جز آنکه در (یک) حکم یکتایی قویتری داریم ، زیرا عاملهای پایا (به خلاف مقسوم‌علیه‌های مقدماتی) را می‌توان به‌وسیلهٔ بخشپذیری به‌طور منحصر به فرد مرتب کرد .

نتیجهٔ ۸.۴ . *فرض کنیم* $\phi : E \to E$ *تبدیلی خطی از فضای برداری* n *بعدی* E *روی میدان* K *باشد .*

(یک) هرگاه ϕ *دارای ماتریس* $A \in Mat_n K$ *نسبت به پایه‌ای باشد ، آنگاه عاملهای پایا [مقسوم‌علیه‌های مقدماتی]* ϕ *عوامل پایای [مقسوم علیه های مقدماتی]* A *می‌باشند .*

(دو) دو ماتریس در $Mat_n K$ *متشابه‌اندا‌گرو فقط اگر دارای عوامل پایای [مقسوم‌علیه‌های مقدماتی] یکسان باشند .*

برهان . تمرین .

تبصره . هرگاه k عنصری از میدان K باشد ، آنگاه ماتریس kI_n مجموع مستقیمی از

ماتریسهای‌همراه 1×1 چندجمله‌ایهای‌تحویل‌ناپذیر $x-k, \ldots, x-k$ است. بنابراین، طبق نتیجهٔ ۷.۴، $x-k, \ldots, x-k$ مقسوم‌علیه‌های مقدماتی kI_n اند. درنتیجه، هرگاه $k_1 \neq k_2$، آنگاه، طبق نتیجهٔ ۸.۴، $k_1 I_n$ و $k_2 I_n$ متشابه نیستند. لذا، اگر K نامتناهی باشد، بی‌نهایت ردهٔ هم‌ارزی متمایز تحت تشابه در $\mathrm{Mat}_n K$ وجود دارد. از آن‌سو، بنابر قضیهٔ ۶.۲، فقط $n+1$ ردهٔ هم‌ارزی متمایز تحت هم‌ارزی در $\mathrm{Mat}_n K$ وجود دارد.

مثال. فرض کنیم E یک فضای‌برداری حقیقی با بعد متناهی بوده و $\phi: E \to E$ تبدیلی خطی با عوامل پایایی چون $q_1 = x^4 - 4x^3 + 5x^2 - 4x + 4 = (x-2)^2(x^2+1) \in \mathbf{R}[x]$ و

$$q_2 = x^7 + 6x^6 + 14x^5 - 20x^4 + 25x^3 - 22x^2 + 12x - 8 = (x-2)^3(x^2+1)^2 \in \mathbf{R}[x]$$

باشد. بنابرقضیهٔ ۶.۴ (یک)، $\dim_K E = 11$ و چندجمله‌ای مینیمال ϕ مساوی q_2 است. تبصره‌های‌بعدازقضیهٔ ۲.۴ نشان‌می‌دهندکه مقسوم‌علیه‌های مقدماتی ϕ در $\mathbf{R}[x]$ عبارتند از x^2+1، $(x^2+1)^2 = x^4 + 2x^2 + 1$، $(x-2)^2 = x^2 - 4x + 4$، $(x-2)^3 = x^3 - 6x^2 + 12x - 8$ و x^2+1. بنابرقضیهٔ ۶.۴، E دو پایه دارد که ماتریسهای ϕ نسبت به‌آنها عبارتند از

$$D = \begin{pmatrix} 0 & 1 & 0 & 0 & & & & & & & \\ 0 & 0 & 1 & 0 & & & & 0 & & & \\ 0 & 0 & 0 & 1 & & & & & & & \\ -4 & 4 & -5 & 4 & & & & & & & \\ & & & & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ & & & & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ & & & & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ & & 0 & & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ & & & & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & & & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & & & & 8 & -12 & 22 & -25 & 20 & -14 & -6 \end{pmatrix},$$

$$M = \begin{pmatrix} 0 & 1 & 0 & & & & & & & & \\ 0 & 0 & 1 & & & & & 0 & & & \\ 8 & -12 & 6 & & & & & & & & \\ & & & 0 & 1 & & & & & & \\ & & & -4 & 4 & & & & & & \\ & & & & & 0 & 1 & 0 & 0 & & \\ & & & & & 0 & 0 & 1 & 0 & & \\ & 0 & & & & 0 & 0 & 0 & 1 & & \\ & & & & & -1 & 0 & -2 & 0 & & \\ & & & & & & & & & 0 & 1 \\ & & & & & & & & & -1 & 0 \end{pmatrix}.$$

ماتریس D به‌شکل کانونی گویا و M به‌شکل کانونی گویای اول است. هرگاه E یک فضای برداری مختلط بوده و $\psi : E \to E$ تبدیلی خطی با همان عاملهای پایای $q_1 = (x-2)^2(x^2+1) \in \mathbf{C}[x]$ و $q_2 = (x-2)^3(x^2+1)^2 \in \mathbf{C}[x]$، چون در $\mathbf{C}[x]$، $x^2+1 = (x+i)(x-i)$، مقسوم علیه‌های مقدماتی ψ در $\mathbf{C}[x]$ عبارتنداز $(x-2)^3$، $(x-2)^2$، $(x+i)^2$، $(x+i)$، $(x-i)^2$، و $(x-i)$. بنابراین، ψ نسبت به پایه‌ای از E دارای ماتریس زیر به شکل کانونی ژردان است:

$$J = \begin{pmatrix} 2 & 1 & 0 & & & & & & & \\ 0 & 2 & 1 & & & & & & & \\ 0 & 0 & 2 & & & & & 0 & & \\ & & & 2 & 1 & & & & & \\ & & & 0 & 2 & & & & & \\ & & & & & -i & 1 & & & \\ & & & & & 0 & -i & & & \\ & & 0 & & & & & -i & & \\ & & & & & & & & i & 1 \\ & & & & & & & & 0 & i \\ & & & & & & & & & & i \end{pmatrix}.$$

تبصره. عوامل پایای ماتریس $A \in \mathrm{Mat}_n K$ در $K[x]$ همان عوامل پایای A در $F[x]$ اند، که در آن F یک توسیع میدان K می‌باشد (تمرین ۶). اما، همانطور که مثال قبل نشان می‌دهد، مقسوم علیه‌های مقدماتی A روی K ممکن است با مقسوم علیه‌های مقدماتی A روی F تفاوت داشته باشد.

این بخش را با روشی برای محاسبهٔ عوامل پایای ماتریس A، و لذا، بنابر نتیجهٔ ۸.۴، هرتبدیل‌خطی که ماتریسش نسبت به پایه‌ای A باشد، خاتمه می‌دهیم. این روش نتیجه‌ای از حکم زیر است.

حکم ۹.۴. *فرض کنیم A یک ماتریس $n \times n$ روی میدان K باشد. در این صورت، ماتریس چندجمله‌ایهای $xI_n - A \in Mat_n K[x]$ (روی $K[x]$) معادل یک ماتریس قطری مانند D با درایه‌های قطری ناصفر $f_1, \ldots, f_n \in K[x]$ است به‌طوری که هر f_i تکین بوده و $f_1 | f_2 | \cdots | f_n$. آن چندجمله‌ایهای f_i که ثابت نیستند عوامل پایای A می‌باشند.*

تبصره. هرگاه K میدان باشد، آنگاه $K[x]$ یک دامنهٔ اقلیدسی است (نتیجهٔ III ۴.۶.).

درنتیجه، برهان زیر همراه با تبصره‌های بعد از حکم ۱۱.۲ نشان می‌دهند که ماتریس D را می‌توان از $xI_n - A$ با رشته‌ای‌متناهی‌ازاعمال سطری و ستونی مقدماتی به دست آورد. لذا، حکم ۹.۴ در واقع روشی ساختنی برای یافتن عوامل پایا به دست می‌دهد. پس‌از برهان مثالی خواهیم آورد.

طرح برهان ۹.۴. فرض کنیم $\phi : K^n \to K^n$ ، K ــ تبدیل‌خطی با ماتریس $A = (a_{ij})$ نسبت به پایهٔ متعارف $\{\varepsilon_i\}$ از K^n باشد. طبق معمول، K^n یک $K[x]$ ــ مدول با ساختار القاشده‌به‌وسیلهٔ ϕ است. همچنین، F یک $K[x]$ ــ مدول‌آزاد به پایهٔ $U = \{u_1, \ldots, u_n\}$ بوده و $\pi : F \to K^n$ همریختی $K[x]$ ــ مدولهای منحصر به فرد باشد که، به‌ازای $i = 1,2, \ldots, n$ ، $\pi(u_i) = \varepsilon_i$ (قضیهٔ IV ۱۰.۲۰). فرض کنیم $\psi : F \to F$ همریختی $K[x]$ ــ مدولهای‌منحصربه‌فرد باشد به‌طوری‌که $\psi(u_i) = xu_i - \sum_{j=1}^{n} a_{ij}u_j$. در این صورت، ماتریس ψ نسبت به پایهٔ U عبارت است از $xI_n - A$.

حکم می‌کنیم که دنبالهٔ $F \xrightarrow{\psi} F \xrightarrow{\pi} K^n \to 0$ از $K[x]$ ــ مدولها کامل است. واضح است که π یک بروریختی $K[x]$ ــ مدولهاست. چون A ماتریس ϕ بوده و ساختار $K[x]$ ــ مدولی K^n به وسیلهٔ ϕ القا می‌شود،

$$\pi(xu_i) = x\pi(u_i) = x\varepsilon_i = \phi(\varepsilon_i) = \sum_{j=1}^{n} a_{ij}\varepsilon_j.$$

درنتیجه، به‌ازای هر i ،

$$\pi\psi(u_i) = \pi\left(xu_i - \sum_{j=1}^{n} a_{ij}u_j\right) = \pi(xu_i) - \sum_j a_{ij}\pi(u_j)$$
$$= \sum_j a_{ij}\varepsilon_j - \sum_j a_{ij}\varepsilon_j = 0,$$

که از آنجا $\operatorname{Im}\psi \subset \operatorname{Ker}\pi$. برای نشان دادن $\operatorname{Ker}\pi \subset \operatorname{Im}\psi$ کافی است ثابت کنیم هر عنصر w از F به شکل $w = \psi(v) + \sum_{j=1}^{n} k_j u_j$ $(v \in F, k_j \in K)$ است. زیرا، در این حالت، هرگاه $w \in \operatorname{Ker}\pi$ ، آنگاه

$$0 = \pi(w) = \pi\psi(v) + \pi(\sum_j k_j u_j) = 0 + \sum_j k_j\varepsilon_j.$$

چون $\{\varepsilon_j\}$ پایه‌ای‌از K^n است، به‌ازای‌هر j ، $k_j = 0$. بنابراین، $w = \psi(v)$ ؛ و درنتیجه،

$\operatorname{Ker}\pi \subset \operatorname{Im}\psi$. چون هر عنصر F مجموعی از جملات به شکل fu_i با $f \in K[x]$ است، کافی است نشان دهیم که به‌ازای هر i و t ، $v_{it} \in F$ ای و $k_i \in K$ ای وجود دارند به طوری‌که $xu_i = \psi(u_i) + \sum_j a_{ij}u_j$. به‌ازای هر i و $t = 1$ ، داریم $x^t u_i = \psi(v_{it}) + \sum_{j=1}^{n} k_j u_j$ ، $(a_{ij} \in K)$. به استقرا عمل کرده، فرض می‌کنیم به‌ازای هر j ، $v_{j,t-1} \in F$ ای و $k_{jr} \in K$ ی وجود دارند به‌طوری‌که $x^{t-1}u_j = \psi(v_{j,t-1}) + \sum_{r=1}^{n} k_{jr}u_r$. در این صورت، به‌ازای هر i ،

$$\begin{aligned} x^t u_i &= x^{t-1}(xu_i) = x^{t-1}(\psi(u_i) + \sum_j a_{ij}u_j) = \psi(x^{t-1}u_i) + \sum_j a_{ij}x^{t-1}u_j \\ &= \psi(x^{t-1}u_i) + \sum_j a_{ij}(\psi(v_{j,t-1}) + \sum_r k_{jr}u_r) \\ &= \psi(x^{t-1}u_i + \sum_j a_{ij}v_{j,t-1}) + \sum_r (\sum_j a_{ij}k_{jr})u_r. \end{aligned}$$

لذا، $x^t u_i = \psi(v_{it}) + \sum_r c_r u_r$ ، که در آن $v_{it} = x^{t-1}u_i + \sum_j a_{ij}v_{j,t-1} \in F$ و $c_r = \sum_j a_{ij}k_{jr} \in K$ و استقرا تمام است. بنابراین، $K^n \to 0 \xrightarrow{\pi} F \xrightarrow{\psi} F \to K^n \to 0$ کامل است؛ و درنتیجه،

$$K^n \cong F/\operatorname{Ker}\pi = F/\operatorname{Im}\psi$$

چون $K[x]$ یک دامنهٔ ایده‌آل اصلی است، حکم ۱۱.۲ نشان می‌دهد که $xI_n - A$ با ماتریس قطری $D = \begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$ معادل است، که در آن r رتبهٔ $xI_n - A$ بوده و L_r یک ماتریس قطری $r \times r$ با درایه‌های قطری ناصفر $f_1, \ldots, f_r \in K[x]$ است به‌طوری که $f_1 | f_2 | \cdots | f_r$. می‌توان فرض کرد هر f_i تکین باشد (در صورت لزوم، بر D اعمال سطری مقدماتی مناسبی انجام دهید). واضح است که دترمینان $|xI_n - A|$ در $K[x]$ یک چندجمله‌ای تکین از درجهٔ n است. بخصوص، $|xI_n - A| \neq 0$. بنابر تعریف ۸.۱ و قضیهٔ ۵.۳ (سه) و (چهار)، $|D|$ مضرب یکه‌ای از $|xI_n - A|$ است، که از آنجا $|D| \neq 0$. درنتیجه، تمام درایه‌های قطری D ناصفرند. لذا $L_r = D$ و $r = n$. چون D با $xI_n - A$ معادل است، D ماتریس ψ نسبت به جفت پایهٔ مرتبی مانند $V = \{v_1, \ldots, v_n\}$ و $W = \{w_1, \ldots, w_n\}$ از F می‌باشد (قضیهٔ ۶.۱). این یعنی به‌ازای هر i ، $\psi(v_i) = f_i w_i$ و $\operatorname{Im}\psi = K[x]f_1w_1 \oplus \cdots \oplus K[x]f_nw_n$. درنتیجه،

$$\begin{aligned} K^n \cong F/\operatorname{Ker}\pi = F/\operatorname{Im}\psi &= \frac{K[x]w_1 \oplus \cdots \oplus K[x]w_n}{K[x]f_1w_1 \oplus \cdots \oplus K[x]f_nw_n} \\ &\cong K[x]w_1/K[x]f_1w_1 \oplus \cdots \oplus K[x]w_n/K[x]f_nw_n \\ &\cong K[x]/(f_1) \oplus \cdots \oplus K[x]/(f_n), \end{aligned}$$

که در آن هر f_i تکین بوده و $f_1 \mid f_2 \mid \cdots \mid f_n$. به‌ازای t ای $(0 \le t \le n)$ ، $f_1 = f_2 = \cdots = f_t = 1_K$ و $f_{t+1}, \ldots, f_n$ غیرثابت‌اند . لذا ، به‌ازای $i \le t$ ،

$$K[x]/(f_i) = K[x]/(1_K) = 0$$

و ، به‌ازای $i > t$ ، $K[x]/(f_i)$ یک $K[x]$ ــ مدول دوری از مرتبهٔ f_i است . بنابراین ، K^n مجموع مستقیم داخلی $K[x]$ــ زیرمدولهای دوری تابی ناصفر (زیر فضاهای ϕ ــ دوری) $E_{t+1}, \ldots, E_n$ به ترتیب از مرتبه‌های $f_{t+1}, \ldots, f_n$ می‌باشد به‌طوری‌که $f_n \mid f_{t+2} \mid \cdots \mid f_{t+1}$. چون ساختار $K[x]$ ــ مدولی K^n به‌وسیلهٔ ϕ القا می‌شود ؛ $0 = f_i E_i = f_i(\phi) E_i$. پس فورا " نتیجه می‌شود که f_i چندجمله‌ای مینیمال $\phi \mid E_i$ است . بنابراین ، طبق قضیهٔ ۲۰۴ ، $f_{t+1}, \ldots, f_n$ عوامل پایای ϕ (و درنتیجه ، A) می‌باشند .

مثال . هرگاه $\phi : \mathbf{Q}^3 \to \mathbf{Q}^3$ تبدیلی خطی بوده و ماتریس ϕ نسبت به پایه‌ای باشد ، آنگاه $A = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$ $xI_3 - A = \begin{pmatrix} x & -4 & -2 \\ 1 & x+4 & 1 \\ 0 & 0 & x+2 \end{pmatrix}$. با انجام اعمال سطری و ستونی مقدماتی مناسب ، نتیجه می‌شود که

$$\begin{pmatrix} x & -4 & -2 \\ 1 & x+4 & 1 \\ 0 & 0 & x+2 \end{pmatrix} \to \begin{pmatrix} 1 & x+4 & 1 \\ x & -4 & -2 \\ 0 & 0 & x+2 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & x+4 & 1 \\ 0 & -4-x(x+4) & -2-x \\ 0 & 0 & x+2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(x+2)^2 & -(x+2) \\ 0 & 0 & x+2 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -(x+2)^2 & 0 \\ 0 & 0 & x+2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+2 & 0 \\ 0 & 0 & (x+2)^2 \end{pmatrix}.$$

بنابراین ، طبق نتیجهٔ ۸۰۴ و حکم ۹۰۴ ، عوامل پایای A و ϕ عبارتند از $x+2$ و $(x+2)^2$ و چندجمله‌ای مینیمال آنها $(x+2)^2$ می‌باشد .

تمرینات

تذکر . E یک فضای برداری n بعدی روی میدان K است مگر خلافش گفته شود .

۱ . هرگاه A و B ماتریسهایی $n \times n$ روی K به ترتیب با چندجمله‌ای‌های مینیمال q_1

و q_2 باشند، آنگاه چندجمله‌ای مینیمال مجموع مستقیم A و B (یک ماتریس $2n \times 2n$) کوچکترین مضرب مشترک q_1 و q_2 می‌باشد.

۲. تبدیل خطی صفر $E \to E$ دارای عوامل پایا [مقسوم‌علیه‌های مقدماتی $q_1 = x, q_2 = x, \ldots, q_n = x$] است.

۳. (آ) فرض کنید a,b,c عناصر متمایزی از K بوده و $D \in \mathrm{Mat}_6 K$ ماتریس قطری با قطر اصلی a,a,a,b,b,c باشد. در این صورت، عوامل پایای D عبارتند از $q_1 = x - a$، $q_2 = (x-a)(x-b)$، و $q_3 = (x-a)(x-b)(x-c)$.

(ب) عوامل پایای هر ماتریس قطری در $\mathrm{Mat}_n K$ را توصیف کنید.

۴. هرگاه q چندجمله‌ای مینیمال تبدیل خطی $\phi : E \to E$ بوده و $\dim_K E = n$، آنگاه $\deg q \leq n$.

۵. چندجمله‌ای مینیمال ماتریس همراه چندجمله‌ای تکین $f \in K[x]$ دقیقاً f است.

۶. فرض کنید F یک توسیع میدان K باشد. عوامل پایای ماتریس $A \in \mathrm{Mat}_n K$ در $K[x]$ همان عوامل پایای A، به عنوان یک ماتریس روی F، در $F[x]$ اند.

[**راهنمایی.** هر K ـ پایه از K^n یک F ـ پایه از F^n است. از تبدیلات خطی استفاده کنید.]

۷. فرض کنید F یک توسیع میدان K باشد. $A,B \in \mathrm{Mat}_n K \subset \mathrm{Mat}_n F$ روی F متشابه‌اند اگر و فقط اگر روی K متشابه باشند [ر.ک. تمرین ۶].

۸. $A \in \mathrm{Mat}_n K$ متشابه یک ماتریس قطری است اگر و فقط اگر مقسوم‌علیه‌های مقدماتی A همه خطی باشند.

۹. هرگاه $A \in \mathrm{Mat}_n K$ پوچ توان باشد (یعنی، به‌ازای $r > 0$ ی، $A^r = 0$)، آنگاه A با ماتریسی متشابه است که تمام درایه‌هایش، جز بعضی از درایه‌های 1_K روی قطر بلافاصله *بالای* قطر اصلی، صفرند.

۱۰. تمام شکلهای کانونی گویای [اول] ماتریس $A \in \mathrm{Mat}_n \mathbf{Q}$ را چنان بیابید که (یک) A ماتریسی 6×6 با چندجمله‌ای مینیمال $(x-2)^2(x+3)$ باشد؛ (دو) A ماتریسی 7×7 با چند جمله‌ای مینیمال $(x^2+1)(x-7)$ باشد. تمام شکلهای کانونی ژردان A را، به عنوان ماتریسی روی $\mathbf{C}$، بیابید.

۱۱. اگر A ماتریس همراه چندجمله‌ای تکین $f \in K[x]$ با $\deg f = n$ باشد، صریحاً نشان دهید که $A - xI_n$ با یک ماتریس قطری متشابه است که قطر اصلی‌اش $1_K, 1_K, \ldots, 1_K, f$

می‌باشد.

۱۲. $A \in \mathrm{Mat}_n K$ خودتوان است اگر $A^2 = A$. نشان دهید دو ماتریس خودتوان در $\mathrm{Mat}_n K$ متشابه‌اند اگر و فقط اگر معادل باشند.

۱۳. یک ماتریس $n \times n$، A با ترانهاده‌اش A^t متشابه است.

۵ چندجمله‌ای مشخص، بردارهای ویژه و مقدارهای ویژه

در این بخش چند پایای دیگر یک تبدیل خطی از یک فضای برداری با بعد متناهی روی یک میدان را بررسی می‌کنیم. چون بعضی از این نتایج به‌طور کلیتر برقرارند، هر وقت میسر بود با مدولهای آزاد از رتبهٔ متناهی روی حلقهٔ تعویضپذیر یکدار کار خواهیم کرد.

هرگاه A یک ماتریس $n \times n$ روی حلقهٔ تعویضپذیر و یکدار K باشد، آنگاه $xI_n - A$ یک ماتریس $n \times n$ روی $K[x]$ است، که از آنجا دترمینان $|xI_n - A|$ عنصری از $K[x]$ می‌باشد. **چندجمله‌ای مشخص ماتریس** A چندجمله‌ای $p_A = |xI_n - A| \in K[x]$ است. واضح است که p_A یک چندجمله‌ای تکین از درجهٔ n است. هرگاه $B \in \mathrm{Mat}_n K$ با A متشابه باشد، مثلاً $B = PAP^{-1}$، آنگاه، چون xI_n در مرکز حلقهٔ $\mathrm{Mat}_n K[x]$ است،

$$\begin{aligned} p_B = |xI_n - B| &= |xI_n - PAP^{-1}| = |P(xI_n - A)P^{-1}| \\ &= |P||xI_n - A||P|^{-1} = |xI_n - A| = p_A; \end{aligned}$$

یعنی، *ماتریسهای متشابه دارای چندجمله‌ای مشخص یکسانند.*

فرض کنیم $\phi : E \to E$ یک درونریختی از K ــ مدول E با رتبهٔ متناهی n باشد (ر.ک. تعریف IV ۸.۲۰ و نتیجهٔ IV ۱۲.۲۰). **چندجمله‌ای مشخص درونریختی** ϕ (که با p_ϕ نموده می‌شود) مساوی p_A تعریف می‌شود، که در آن A ماتریسی از ϕ نسبت به یک پایهٔ مرتب است. چون، بنابر نتیجهٔ ۷.۱، هر دو ماتریس نمایش ϕ متشابه‌اند، p_ϕ از انتخاب A مستقل است.

لم ۱۰.۵. (یک) *هرگاه* $A_1, A_2, \ldots, A_r$ *ماتریسهایی مربعی (به اندازه‌های مختلف) روی حلقهٔ تعویضپذیر و یکدار* K *بوده و* $p_i \in K[x]$ *چندجمله‌ای مشخص* A_i *باشد، آنگاه* $p_1 p_2 \cdots p_r \in K[x]$ *چندجمله‌ای مشخص ماتریس مجموع مستقیم* $A_1, A_2, \ldots, A_r$ *می‌باشد.*

(دو) *ماتریس همراه* C *از چندجمله‌ای تکین* $f \in K[x]$ *دارای چندجمله‌ای مشخص* f *است.*

طرح برهان. (یک) هرگاه $A \in \mathrm{Mat}_n K$ و $B \in \mathrm{Mat}_m K$، آنگاه

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & I_m \end{pmatrix}\begin{pmatrix} I_n & 0 \\ 0 & B \end{pmatrix}$$

، کـــه از آنجا $\begin{vmatrix} A & 0 \\ 0 & B \end{vmatrix} = \begin{vmatrix} A & 0 \\ 0 & I_m \end{vmatrix}\begin{vmatrix} I_n & 0 \\ 0 & B \end{vmatrix} = |A||B|$.

حال استقرا نشان می‌دهدکه دترمینان یک مجموع مستقیم از ماتریسهای $B_1, \ldots, B_k$ مساوی $|B_1||B_2|\cdots|B_k|$ است. (دو) برای نشان دادن اینکـه f چندجمله‌ای مشخص C است، $|xI_n - C|$ را نسبت به سطر آخر بسط دهید.

قضیهٔ ۲۰۵. *فرض کنیم $\phi : E \to E$ تبدیلی خطـی از یک فضای برداری n بعدی روی میدان K با چندجمله‌ای مشخـص $p_\phi \in K[x]$، چندجمله‌ای مینیمال $q_\phi \in K[x]$، و عوامل پایای $q_1, \ldots, q_t \in K[x]$ باشد.*

(یک) چندجمله‌ای مشخص برابر با حاصلضرب عوامل پایاست؛ یعنی،

$$p_\phi = q_1 q_2 \cdots q_t = q_1 q_2 \cdots q_{t-1} q_\phi$$

(دو) (کیلی ــ هامیلتون[1]) ϕ ریشهٔ چندجمله‌ای مشخص خود است؛ یعنی، $p_\phi(\phi) = 0$.

(سه) یک چندجمله‌ای تحـویل‌ناپذیر در $K[x]$، p_ϕ را عاد می‌کند اگر و فقط اگر q_ϕ را عاد کند.

نتایج (یک) تا (سه) نعل به نعل برای هر ماتریس $A \in Mat_n K$ برقرارند.

برهان. بنابر قضیهٔ ۶.۴، ϕ دارای پایه‌ای است که ϕ نسبت به آن دارای ماتریس D است که مجموع مستقیم ماتریسهای همراه $q_1, \ldots, q_t$ می‌باشد. بنابراین، طبق لم ۱۰۵، $p_\phi = p_D = q_1 q_2 \cdots q_t$. به علاوه، طبق قضیهٔ ۲۰۴، $q_\phi = q_t$، که از آنجا $p_\phi(\phi) = 0$، زیرا $q_\phi(\phi) = 0$. (سه) فـورا" از (یک) و اینکـه $q_1 \mid q_2 \mid \cdots \mid q_t$ نتیجه می‌شود. احکام مشابه در باب $A \in \mathrm{Mat}_n K$ را می‌توان بـه همین نحو، با استفاده از نتایج ۷۰۴ و ۸۰۴، ثابت کرد.

تبصره. قضیهٔ کیلی ــ هامیلتون (قضیهٔ ۲۰۵ (دو)) روی هر حلقهٔ تعویضپذیر یکدار معتبر است (تمرین ۲).

تعریف ۳۰۵. فرض کنیم $\phi : E \to E$ تبدیلی خطـی از فضای برداری E روی میدان K

1. Hamilton

باشد. بردار ناصفر $u \in E$ یک **بردار ویژه** (یا **بردار مشخص** یا **بردار حقیقی**) ϕ است اگر به‌ازای $k \in K$ ای، $\phi(u) = ku$. عنصر $k \in K$ یک **مقدار ویژه** (یا **مقدار حقیقی** یا **مقدار مشخص**) ϕ است اگر به‌ازای $u \in E$ ای ناصفر، $\phi(u) = ku$.

ممکن است دو بردار ویژهٔ متمایز (حتی مستقل خطی) یک مقدار ویژه داشته باشند. از آن سو، مجموعه‌ای از بردارهای ویژه که مقادیر ویژهٔ نظیرشان همه متمایزند لزوماً مستقل خطی می‌باشد (تمرین ۸).

قضیهٔ ۴۰۵. *فرض کنیم $\phi: E \to E$ تبدیلی خطی از فضای برداری با بعد متناهی E روی میدان K باشد. در این صورت، مقادیر ویژهٔ ϕ ریشه‌های چندجمله‌ای مشخص p_ϕ از ϕ در K می‌باشند.*

تبصره. چندجمله‌ای مشخص $p_\phi \in K[x]$ لازم نیست در K ریشه داشته باشد، که در این صورت ϕ مقدار ویژه یا بردار ویژه ندارد.

طرح برهان ۴۰۵. فرض کنیم A ماتریس ϕ نسبت به‌پایهٔ مرتبی باشد. هرگاه $k \in K$، آنگاه $kI_n - A$ ماتریس $k1_E - \phi$ نسبت به‌همان پایه است. هرگاه به‌ازای $u \in E$ ی ناصفری $\phi(u) = ku$، آنگاه $(k1_E - \phi)(u) = 0$، که از آنجا $k1_E - \phi$ یک تکریختی نیست. بنابراین، $kI_n - A$ معکوسپذیر نیست (لم ۵۰۱)؛ و درنتیجه، بنابر حکم ۷۰۳ یا تمرین ۶۰۳، $|kI_n - A| = 0$. لذا، k ریشه‌ای از $p_\phi = |xI_n - A|$ است. به عکس، هرگاه k ریشه‌ای از p_ϕ باشد، آنگاه $|kI_n - A| = 0$. درنتیجه، طبق لم ۵۰۱ و حکم ۷۰۳ (یا تمرین ۶۰۳)، $k1_E - \phi$ یکریختی نیست. چون E بابعد متناهی است، $k1_E - \phi$ تکریختی نیست (تمرین IV ۱۴۰۲۰). بنابراین، عنصر ناصفری مانند $u \in E$ هست به‌طوری‌که $(k1_E - \phi)(u) = 0$، که از آنجا $\phi(u) = ku$ و k یک مقدار ویژهٔ ϕ می‌باشد.

هرگاه $k \in K$ یک مقدار ویژهٔ درونریختی ϕ از K ــ فضای برداری E باشد، آنگاه به آسانی معلوم می‌شود که $C(\phi,k) = \{v \in E \mid \phi(v) = kv\}$ زیرفضای ناصفری از E است؛ $C(\phi,k)$ **فضای ویژه** یا **فضای مشخص** k نام دارد.

قضیهٔ ۵۰۵ . *فرض کنیم $\phi: E \to E$ تبدیلی خطی از فضای برداری با بعد متناهی E روی میدان K باشد . در این صورت ، ϕ یک ماتریس قطری D نسبت به پایهٔ مرتبی از E است اگروفقط اگر بردارهای ویژهٔ ϕ ، E را بپیمایند . در این حالت ، درایه‌های قطری D مقادیر ویژهٔ ϕ بوده‌و هر مقدار ویژهٔ $k \in K$ به تعداد $\dim_K C(\phi,k)$ بار روی قطر ظاهر می‌شود .*

برهان . بنابر قضیهٔ IV ۵۰۲۰ ، بردارهای ویژهٔ ϕ ، E را می‌پیمایند اگر و فقط اگر E پایه‌ای مرکب از بردارهای ویژه داشته باشد . واضح است که $U = \{u_1, \ldots, u_n\}$ پایه‌ای از بردارهای ویژه با مقادیر ویژهٔ $k_1, \ldots, k_n \in K$ است اگر و فقط اگر ماتریس ϕ نسبت به U ماتریس قطری D با قطر اصلی $k_1, k_2, \ldots, k_n$ باشد . در این حالت ، فرض کنیم $v = \sum_{i=1}^{n} r_i u_i$ یک بردارویژهٔ ϕ با خاصیت $\phi(v) = kv$ باشد . چون U مستقل‌خطی بوده‌و $kv = \phi(v) = \sum_{i=1}^{n} r_i \phi(u_i) = \sum_{i=1}^{n} r_i k_i u_i$ ، به‌ازای هر i داریم $kr_i = r_i k_i$. لذا ، به‌ازای هر i که $r_i \neq 0$ ، $k = k_i$ (چون $v \neq 0$ ، دست‌کم یک $r_i \neq 0$) . بنابراین ، $k_1, \ldots, k_n$ تنها مقادیر ویژهٔ ϕ می‌باشند . به علاوه ، هرگاه k یک مقدار ویژهٔ ϕ باشد که t بار روی قطر D ظاهر می‌شود و $u_{i_1}, \ldots, u_{i_t}$ عناصری‌از U باشند که مقدار ویژهٔ k دارند ، آنگاه این استدلال نشان می‌دهد که $\{u_{i_1}, \ldots, u_{i_t}\}$ ، $C(\phi,k)$ را می‌پیماید . چون $\{u_{i_1}, \ldots, u_{i_t}\}$ مستقل‌خطی‌است ، پس پایه‌ای‌از $C(\phi,k)$ است . بنابراین ، $\dim_K C(\phi,k) = t$.

مقادیر ویژه و بردارهای ویژهٔ یک ماتریس $n \times n$ مانند A روی میدان K به‌ترتیب با مقادیر ویژه و بردارهای ویژهٔ تبدیل خطی منحصر به فرد $\phi: K^n \to K^n$ که ماتریس‌آن نسبت به‌پایه‌متعارف A است‌تعریف می‌شوند . قضیهٔ ۴۰۵ نشان می‌دهد که مقادیر ویژهٔ A مقادیر ویژهٔ یک درونریختی ازیک فضای برداری n بعدی روی K است که ماتریس‌آن نسبت به پایه‌ای A می‌باشد .

این بخش را بـا بحث کوتاهی از پایای دیگری از یک ماتریس تحت تشابه به پایان می‌بریم .

حکم ۶۰۵ . *فرض کنیم K حلقه‌ای‌تعویضپذیرویکدار باشد . همچنین ، ϕ یک درونریختی*

از یک K *ـ مدول آزاد با رتبهٔ* n *بوده و* $A = (a_{ij}) \in Mat_n K$ *ماتریس* ϕ *نسبت به پایهٔ مرتبی باشد. هرگاه چندجمله‌ای مشخص* ϕ *و* A *مساوی*

$$p_\phi = p_A = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in K[x]$$

باشد، آنگاه $(-1)^n c_0 = |A|$ *و* $-c_{n-1} = a_{11} + a_{22} + \cdots + a_{nn}$.

برهان. بنابر قضیهٔ ۵۰۳ (هشت)، $c_0 = p_\phi(0) = |0I_n - A| = |-A| = (-1)^n|A|$. $p_\phi = |xI_n - A|$ را نسبت به سطر اول بسط می‌دهیم. یک جملهٔ این بسط عبارت است از

$$(x - a_{11})(x - a_{22})\cdots(x - a_{nn}) = x^n - (a_{11} + a_{22} + \cdots + a_{nn})x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$$

که در آن $b_i \in K$. هیچ جملهٔ دیگر این بسط شامل جمله‌ای با عامل x^{n-1} نیست، که از آنجا $-c_{n-1} = a_{11} + \cdots + a_{nn}$.

فرض کنیم K حلقه‌ای تعویضپذیر و یکدار باشد. *اثر ماتریس* $A = (a_{ij})$، $n \times n$ روی K عبارت‌است از $a_{11} + a_{22} + \cdots + a_{nn} \in K$ و با $\mathrm{Tr}A$ نموده می‌شود. *اثر درونریختی* ϕ از یک K ـ مدول آزاد با رتبهٔ n (که با $\mathrm{Tr}\phi$ نموده می‌شود) عبارت است از $\mathrm{Tr}A$، که در آن A ماتریس ϕ نسبت به پایهٔ مرتبی می‌باشد. چون $p_\phi = p_A$ مستقل از ماتریس A است، بنابرحکم ۶۰۵، $\mathrm{Tr}\phi$ نیز چنین‌است. بنابر نتیجهٔ ۷۰۱ (یا استدلال مستقیم آسانی با استفاده از قسمت (سه) زیر)، ماتریسهای متشابه‌اثرهای یکسانی دارند. به‌آسانی معلوم می‌شود که به‌ازای هر $A, B \in \mathrm{Mat}_n K$ و $k \in K$،

(یک) $\mathrm{Tr}(A + B) = \mathrm{Tr}A + \mathrm{Tr}B$؛

(دو) $\mathrm{Tr}(kA) = k\mathrm{Tr}A$؛

(سه) $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

ارتباط بین اثرتعریف‌شده دراینجا و تابع اثر نظریهٔ گالوا (تعریف ۱۰۷۰۷) در تمرین ۹ مطرح شده‌است.

تمرینات

تذکر. K یک حلقهٔ تعویضپذیر و یکدار است مگر خلافش گفته شود.

۱. مستقیما "ثابت کنید یک ماتریس روی K و ترانهادهٔ آن دارای چندجمله‌ای مشخص یکسانند.

۲. (کیلی ـ هامیلتون). هرگاه ϕ یک‌درونریختی K ـ مدول آزاد E با رتبهٔ متناهی

باشد، آنگاه $p_\phi(\phi) = 0$. [**راهنمایی.** هرگاه A ماتریس ϕ بوده‌و $B = xI_n - A$ ، آنگاه، در $\mathrm{Mat}_n K[x]$ ، $B^\sigma B = |B| I_n = p_\phi I_n$. هرگاه E یک $K[x]$ ـ مدول با ساختار القا شده به وسیلهٔ ϕ و ψ درونریختی $K[x]$ ـ مدولهای $E \to E$ با ماتریس B باشد، آنگاه به‌ازای هر $u \in E$ ، $\psi(u) = xu - \phi(u) = \phi(u) - \phi(u) = 0$.]

۳ . هرگاه A یک ماتریس $n \times m$ روی K و B یک ماتریس $m \times n$ روی K باشد، آنگاه $x^m p_{AB} = x^n p_{BA}$. به علاوه، هرگاه $m = n$ ، آنگاه $p_{AB} = p_{BA}$.

[**راهنمایی.** فرض‌کنید C, D ماتریسهای $(m+n) \times (m+n)$ زیرروی $K[x]$ باشند:

$$D = \begin{pmatrix} I_n & 0 \\ -B & xI_m \end{pmatrix} \quad \text{و} \quad C = \begin{pmatrix} xI_n & A \\ B & I_m \end{pmatrix}$$

و توجه کنید که $|CD| = |DC|$.]

۴ . (آ) سه ماتریس 3×3 روی $\mathbf{Q}$ نشان دهید که هیچ دوتای آنها متشابه نبوده و 2 ـ تنها مقدارویژهٔ هر ماتریس باشد.

(ب) یک ماتریس 4×4 نشان دهید که مقادیر ویژه‌اش روی $\mathbf{R}$ مساوی ± 1 بوده‌و مقادیر ویژه‌اش روی $\mathbf{C}$ برابر ± 1 و $\pm i$ باشند.

۵ . فرض کنید K میدان بوده و $A \in \mathrm{Mat}_n K$.

(آ) 0 یک مقدار ویژهٔ A است اگر و فقط اگر A معکوسپذیر نباشد.

(ب) هرگاه $k_1, \ldots, k_r \in K$ مقادیر ویژهٔ (نه لزوما " متمایز) A بوده و $f \in K[x]$ ، آنگاه $f(A) \in \mathrm{Mat}_n K$ دارای مقادیر ویژهٔ $f(k_1), \ldots, f(k_r)$ می‌باشد.

۶ . هرگاه ϕ و ψ درونریختیهایی‌ازیک فضای برداری با بعد متناهی روی میدان به‌طور جبری بستهٔ K باشند به‌طوری‌که $\phi\psi = \psi\phi$ ، آنگاه ϕ و ψ بردارویژهٔ مشترکی خواهند داشت.

۷ . (آ) فرض کنید ϕ و ψ درونریختیهایی از فضای برداری با بعد متناهی E باشند به‌طوری‌که $\phi\psi = \psi\phi$. هرگاه E پایه‌ای‌از بردارهای‌ویژهٔ ϕ و پایه‌ای از بردارهای ویژهٔ ψ داشته‌باشد، آنگاه E یک پایه مرکب از بردارهای ویژه برای هر دوی ϕ و ψ دارد.

(ب) قسمت (آ) را به عنوان حکمی در باب ماتریسهای متشابه با یک ماتریس قطری تعبیر کنید.

۸ . فرض کنید $\phi : E \to E$ تبدیلی خطی ازفضای برداری E روی میدان K باشد. هرگاه

U مجموعه‌ای از بردارهای ویژهٔ ϕ باشد که مقادیر ویژهٔ نظیرشان همه متمایزند، آنگاه U مستقل خطی می‌باشد. [**راهنمایی.** اگر U وابستهٔ خطی می‌بود، رابطه‌ای چون $r_1u_1 + \cdots + r_tu_t = 0$ $(u_i \in U; 0 \neq r_i \in K)$ با t مینیمال وجود می‌داشت. تبدیل $k_1 1_E - \phi$ را، که در آن $\varphi(u_1) = k_1u_1$، به کار برده و به تناقض برسید.]

۹. فرض کنید F یک توسیع میدان از میدان K بوده و $u \in F$. همچنین، $\phi : F \to F$ درونریختی فضای برداری F باشد که با $v \mapsto uv$ داده می‌شود.

(آ) در این صورت، $\mathrm{Tr}\phi$ اثر u، یعنی $T_K^F(u)$، با تعریف ۱۰۷۰ V است. [**راهنمایی.** ابتدا به حالت $F = K(u)$ بپردازید].

(ب) دترمینان ϕ مساوی نرم u، یعنی $N_K^F(u)$، است.

۱۰. فرض کنید K میدان بوده و $A \in \mathrm{Mat}_n K$.

(آ) هرگاه A پوچتوان باشد (یعنی، به‌ازای m ی، $A^m = 0$)، آنگاه، به‌ازای هر $r > 1$، $\mathrm{Tr}A^r = 0$. [**راهنمایی.** چندجمله‌ای مینیمال A^r به شکل x^t بوده و A^r با ماتریسی به شکل گویا یا به شکل کانونی ژردان متشابه است.]

(ب) هرگاه $\mathrm{char}\, K = 0$ و، به‌ازای هر $r \geq 1$، $\mathrm{Tr}A^r = 0$، آنگاه A پوچتوان است.

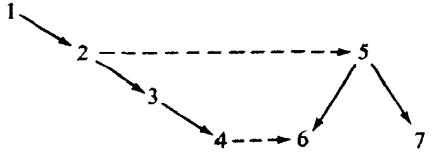
۸

حلقه‌های تعویضپذیر و مدولها

بخش اعظم این فصل مقدمهٔ کوتاهی است بر آنچه اغلب جبر تعویضپذیر نامیده می‌شود. بحث را با شرایط زنجیری (بخش ۱) و ایده‌آلهای اول (بخش ۲)، که هر دو نقش مهمی در بررسی حلقه‌های تعویضپذیر دارند، آغاز می‌کنیم. در بخش ۱ عملاً "هیچ قید تعویضپذیری اعمال نمی‌شود، زیرا این مطالب در مطالعهٔ حلقه‌های دلخواه (فصل نه) نیز لازمند.

نظریهٔ حلقه‌های تعویضپذیر طرح آشنایی دارد: سعی می‌کنیم برای حلقه‌هایی که، لااقل در شکل تعمیم یافته، دارای خواصی هستند که سودمندی آنها در حلقه‌های معروف به ثبوت رسیده، یک نظریهٔ ساختاری به دست آوریم. لذا، در بخشهای ۲ و ۳، تجزیهٔ اولیهٔ ایده‌آلها (مشابه تجزیهٔ عناصر در یک دامنهٔ صحیح) را مطرح می‌کنیم. سپس حلقه‌هایی نظیر دامنه‌های ددکیند[1] (بخش ۶) و حلقه‌های نوتری (بخش ۴) را مطالعه می‌کنیم که در بعضی از خواص مطلوب حلقهٔ اعداد صحیح سهیم‌اند. تحلیل دامنه‌های ددکیند به معلوماتی از توسیع حلقه‌ها نیاز دارد (بخش ۵). این اطلاعات در اثبات قضیهٔ صفرهای هیلبرت[2] (بخش ۷) نیز به کار می‌روند، که نتیجهٔ کلاسیک مشهوری است در رابطه با ایده‌آلهای حلقهٔ چندجمله‌ای $K[x_1, \ldots, x_n]$.

تمام حلقه‌ها، جز در بخش ۱، تعویضپذیرند. ارتباط تقریبی بخشهای این فصل (تحت شرایط زیر) بدین قرار است:



1. Dedekind
2. Hilbert

سهم شکسته‌ٔ $B \leftarrow\!\!- A$ مبین‌آن است که نتایج بخش A گاهی در بخش B به کار می‌روند، ولی بخش B اساسا" از بخش A مستقل است. بخش ۱ برای بخش ۵ لازم نیست، ولی برای بخش ۴ ضرورت دارد. فقط یک نتیجهٔ مهم در بخش ۴ هست که به بخشهای ۲ و ۳ وابسته‌است. این بستگی را می‌توان با استفاده از برهانی دیگر، که در تمرینات ذکر شده، حذف کرد.

۱ شرایط زنجیری

در این بخش نکات اساسی مربوط به شرایط زنجیر افزایشی و کاهشی مربوط به مدولها و حلقه‌ها را که در این فصل و فصل نه لازم می‌شوند خلاصه می‌کنیم. ***حلقه‌ها تعویضپذیر فرض نمی‌شوند و لزوما" یکدار نیستند.***

تعریف ۱۰۱. گوییم مدول A در ***شرط زنجیر افزایشی*** **(ACC)** ***برزیرمدولها*** صدق می‌کند (یا ***نوتری*** است) اگر به‌ازای هر زنجیر $A_1 \subset A_2 \subset A_3 \subset \cdots$ از زیرمدولهای A، عددی صحیح مانند n باشد به‌طوری‌که به‌ازای هر $i \geq n$، $A_i = A_n$.

گوییم مدول B در ***شرط زنجیر کاهشی*** **(DCC)** ***بر زیرمدولها*** صدق می‌کند (یا ***آرتینی***) است اگر به‌ازای هر زنجیر $B_1 \supset B_2 \supset B_3 \supset \cdots$ از زیرمدولهای B، عددی صحیح مانند m باشد به‌طوری‌که به‌ازای هر $i \geq m$، $B_i = B_m$.

مثال. Z ـ مدول (گروه آبلی) Z در شرط زنجیر افزایشی صدق می‌کند ولی در شرط زنجیر کاهشی برزیرمدولها صدق نمی‌کند (تمرین II ۵۰۳۰). Z ـ مدول $Z(p^\infty)$ در شرط زنجیر کاهشی صدق می‌کند ولی در شرط زنجیر افزایشی صدق نمی‌کند (تمرین II ۱۳۰۳۰).

هرگاه حلقهٔ R را یک مدول چپ [راست] روی خودش درنظر بگیریم، آنگاه به‌آسانی معلوم می‌شود که زیرمدولهای R دقیقا" ایده‌آلهای چپ [راست] R می‌باشند. درنتیجه، در این حالت معمولا" از شرایط زنجیری روی ایده‌آلهای چپ و راست، به جای زیرمدولها، صحبت می‌شود.

تعریف ۲۰۱. حلقهٔ R ***نوتری چپ*** [***راست***] است اگر R در شرط زنجیر افزایشی بر ایده‌آلهای چپ [راست] صدق کند. گوییم R ***نوتری*** است اگر نوتری چپ و راست باشد.

حلقهٔ R **آرتینی چپ** [*راست*] است اگر R درشرط زنجیر کاهشی بر ایده‌آلهای چپ [راست] صدق کند. گوییم R **آرتینی** است اگر آرتینی چپ و راست باشد.

به‌عبارت دیگر، حلقهٔ R نوتری (چپ یا راست) است اگر R ــ مدول نوتری (چپ یا راست) باشد، و به همین ترتیب در مورد آرتینی. درنتیجه، تمام تعاریف و نتایج زیر در مورد مدولها که در شرط زنجیر افزایشی یا کاهشی بر زیرمدولها صدق می‌کنند، نعل به نعل، در مورد حلقه‌های نوتری یا آرتینی (چپ یا راست) به کار می‌روند.

چند مثال. حلقهٔ بخشی D هم نوتری است هم آرتینی، زیرا تنها ایده‌آلهای چپ و راست آن D و 0 اند (تمرین III ۷.۲۰). هر حلقهٔ ایده‌آل اصلی تعویضپذیر نوتری است (لم III ۶.۳۰)؛ ازجمله حالات خاص $\mathbf{Z}$ ، Z_n ، و $F[x]$ اند که F میدان می‌باشد.

مثال. حلقهٔ $\mathrm{Mat}_n D$ مرکب از تمام ماتریسهای $n \times n$ روی یک حلقهٔ بخشی هم نوتری است هم آرتینی (نتیجهٔ ۱۲.۱ زیر).

چند تبصره. یک حلقهٔ نوتری [آرتینی] راست لازم نیست نوتری [آرتینی] چپ باشد (تمرین ۱). تمرین II ۵.۳۰ نشان می‌دهد که یک حلقهٔ نوتری لزوماً آرتینی نیست. با اینحال، هر حلقهٔ یکدار آرتینی چپ [راست] یکدار نوتری چپ [راست] می‌باشد (تمرین IX ۱۳.۳۰ زیر).

در بخش ۷ آشنایی، عنصر ماکزیمال در مجموعهٔ جزئی مرتب $(C,\leq)$ تعریف شد. **عنصر مینیمال** به همین نحو تعریف می‌شود: $b \in C$ مینیمال است اگر به‌ازای هر $c \in C$ **که با** b **قیاسپذیر است**، $b \leq c$. توجه‌کنید که لازم نیست به‌ازای **هر** $c \in C$ ، $b \leq c$. به علاوه، C ممکن است عنصر مینیمال بسیار داشته باشد یا هیچ عنصری از این نوع نداشته باشد.

تعریف ۳.۱. گوییم مدول A در *شرط ماکزیمال* [*شرط مینیمال*] *برزیرمدولها* صدق می‌کند اگر هرمجموعهٔ ناتهی از زیرمدولهای A شامل عنصر ماکزیمال [مینیمال] (نسبت به‌شمول نظریهٔ مجموعه‌ها) باشد.

قضیهٔ ۴.۱ . *مدول A در شرط زنجیر افزایشی [کاهشی] بر زیر مدولها صدق می‌کند اگر و فقط اگر در شرط ماکزیمال [مینیمال] بر زیرمدولها صدق نماید .*

برهان . فرض کنیم A در شرط مینیمال بر زیرمدولها صدق کرده و $A_1 \supset A_2 \supset \cdots$ یک زنجیر از زیرمدولها باشد . در این صورت ، مجموعهٔ $\{A_i \mid i \geq 1\}$ عنصر مینیمال ، مثلاً A_n ، دارد . درنتیجه ، به‌ازای $i \geq n$ ، طبق فرض داریم $A_n \supset A_i$ و ، طبق مینیمالی ، $A_n \subset A_i$ ، که از آنجا ، به‌ازای هر $i \geq n$ ، $A_i = A_n$. بنابراین ، A در شرط زنجیر کاهشی صدق می‌کند .

به‌عکس ، فرض کنیم A در شرط زنجیر کاهشی صدق کند ، و S مجموعه‌ای ناتهی از زیرمدولهای A باشد . در این صورت ، $B_0 \in S$ ی وجود دارد . هرگاه S عنصر مینیمال نداشته باشد ، آنگاه ، به‌ازای هرزیرمدول B در S ، دست‌کم یک زیرمدول B' در S هست به‌طوری‌که $B \supsetneq B'$. به‌ازای هر B در S ، یکی از این B' ها را اختیار می‌کنیم (اصل انتخاب) . این انتخاب تابع $f : S \to S$ را با $B \mapsto B'$ تعریف می‌کند . بنابر قضیهٔ بازگشتی ۲.۶ در آشنایی (با $f = f_n$ به‌ازای هر n) ، تابعی مانند $\varphi : \mathbf{N} \to S$ وجود دارد به‌طوری‌که

$$\varphi(0) = B_0 \quad \text{و} \quad \varphi(n+1) = f(\varphi(n)) = \varphi(n)' \ .$$

لذا ، هرگاه $B_n \in S$ نمایش $\varphi(n)$ باشد ، آنگاه دنباله‌ای مانند $B_0, B_1, \ldots$ وجود دارد به طوری‌که $B_0 \supsetneq B_1 \supsetneq B_2 \supsetneq \cdots$. این امر با شرط زنجیر کاهشی در تضاد است . بنابراین ، S باید عنصر مینیمال داشته باشد ؛ درنتیجه ، A در شرط مینیمال صدق می‌نماید .

اثبات در مورد شرایط زنجیر افزایشی و ماکزیمال به همین نحو است .

قضیهٔ ۵.۱ . *فرض کنیم $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ یک دنبالهٔ کامل کوتاه از مدولها باشد . در این صورت ، B در شرط زنجیر افزایشی [کاهشی] بر زیرمدولها صدق می‌کند اگر و فقط اگر A و C در آن صدق نمایند .*

طرح برهان . هرگاه B در شرط زنجیر افزایشی صدق کند ، آنگاه زیرمدول آن $f(A)$ نیز چنین است . بنابر کامل بودن دنباله ، A با $f(A)$ یکریخت است ؛ درنتیجه ، A در شرط زنجیر افزایشی صدق می‌کند . هرگاه $C_1 \subset C_2 \subset \cdots$ زنجیری از زیرمدولهای C باشد ، آنگاه $g^{-1}(C_1) \subset g^{-1}(C_2) \subset \cdots$ زنجیری از زیرمدولهای B خواهد بود .

بنابراین، n ی وجـــــــــــــــــــــودداردبه‌طـــــــــــــــــــــوری‌که‌به‌ازای‌هر $i \geq n$ ، $g^{-1}(C_i) = g^{-1}(C_n)$. چون g طبق کامل بودن برووریختی است، نتیجه می‌شود که به‌ازای هر $i \geq n$ ، $C_i = C_n$. بنابراین، C در شرط زنجیر افزایشی صدق می‌کند.

فرض کنیم A و C در شرط زنجیر افزایشی صدق کنند و $B_1 \subset B_2 \subset \cdots$ زنجیری از زیرمدولهای B باشد. به‌ازای هر i قرار می‌دهیم

$$A_i = f^{-1}(f(A) \cap B_i) \quad \text{و} \quad C_i = g(B_i) .$$

فرض کنیم $f_i = f \mid A_i$ و $g_i = g \mid B_i$. تحقیق کنید که دنبالهٔ زیر به‌ازای هر i کامل است:

$$0 \to A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \to 0.$$

تحقیق کنید که $A_1 \subset A_2 \subset \cdots$ و $C_1 \subset C_2 \subset \cdots$. طبق فرض، عدد صحیحی مانند n هست به‌طوری‌که، به‌ازای هر $i \geq n$ ، $A_i = A_n$ و $C_i = C_n$. به‌ازای هر $i \geq n$ یک نمودار تعویضپذیر با سطرهای کامل وجود دارد:

$$\begin{array}{ccccccccc} 0 & \to & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \to & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta_i} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \to & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \to & 0, \end{array}$$

که در آن α و γ نگاشتهای همانی مربوطه و β_i نگاشت شمول است. لم پنج کوتاه IV ۱۷.۱۰ ایجاب می‌کندکه β_i نگاشت‌همانی‌باشد؛ درنتیجه، B در شرط زنجیرافزایشی صدق می‌کند. اثبات در مورد شرط زنجیر کاهشی به همین نحو است.

نتیجهٔ ۶.۱ . *هرگاه A زیرمدولی از مدول B باشد، آنگاه B در شرط زنجیر افزایشی [کاهشی] صدق می‌کند اگر و فقط اگر A و B/A در آن صدق کنند.*

برهان. قضیهٔ ۵.۱ را بر دنبالهٔ $0 \to A \xrightarrow{\subseteq} B \to B/A \to 0$ اعمال کنید.

نتیجهٔ ۷.۱ . *هرگاه $A_1, \ldots, A_n$ مدول باشند، آنگاه مجموع مستقیم $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ در شرط زنجیر افزایشی [کاهشی] بر زیرمدولها صدق می‌کند اگر و فقط اگر هر A_i در آن صدق کند.*

طرح برهان. از استقرا بر n استفاده‌کنید. اگر $n = 2$ ، قضیهٔ ۵۰۱ را در مورد دنبالهٔ $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$ به کار برید.

قضیهٔ ۸۰۱. *هرگاه R یک‌حلقهٔ یکدار نوتری [آرتینی] چپ باشد، آنگاه هر R ــ مدول چپ یکانی و با تولید متناهی A در شرط زنجیر افزایشی [کاهشی] بر زیرمدولها صدق خواهد کرد.*

حکم مشابهی با "راست" به جای "چپ" برقرار است.

برهان ۸۰۱. هرگاه A با تولید متناهی باشد، آنگاه، بنابر نتیجهٔ IV ۲۰۲۰، یک R ــ مدول آزاد F با پایهٔ متناهی و یک بروریختی $\pi : F \to A$ وجود دارند. چون، بنابر قضیهٔ IV ۱۰۲۰، F مجموع مستقیمی از چند نسخه از R است، F طبق نتیجهٔ ۷۰۱ نوتری [آرتینی] چپ‌می‌باشد. بنابراین، طبق نتیجهٔ ۶۰۱، $A \cong F/\mathrm{Ker}\,\pi$ نوتری [آرتینی] می‌باشد.

ذیلاً توصیفی از شرط زنجیر افزایشی می‌آید که مشابهی برای شرط زنجیر کاهشی ندارد.

قضیهٔ ۹۰۱. *مدول A در شرط زنجیر افزایشی بر زیرمدولها صدق می‌کند اگر و فقط اگر هر زیرمدول A با تولید متناهی باشد. بخصوص، حلقهٔ تعویضپذیر R نوتری است اگر و فقط اگر هر ایده‌آل R با تولید متناهی باشد.*

برهان. (⇐) اگر B زیرمدولی از A باشد، S را مجموعهٔ تمام زیرمدولهای با تولید متناهی B می‌گیریم. چون S ناتهی است $(0 \in S)$، طبق قضیهٔ ۴۰۱، S شامل عنصر ماکزیمالی مانند C است. C به وسیلهٔ تعدادی متناهی عنصر مانند $c_1, c_2, \ldots, c_n$ تولید می‌شود. به‌ازای هر $b \in B$، فرض کنیم D_b زیرمدولی از B باشدکه‌به‌وسیلهٔ $b, c_1, c_2, \ldots, c_n$ تولید می‌شود. در این صورت، $D_b \in S$ و $C \subset D_b$. چون C ماکزیمال است، به‌ازای هر $b \in B$، $D_b = C$، که از آنجا، به‌ازای هر $b \in B$، $b \in D_b = C$ و $B \subset C$. چون طبق

ساخت $B = C$ ، $C \subset B$ ؛ و لذا ، B با تولید متناهی است .

($\Rightarrow$) زنجیر $A_1 \subset A_2 \subset A_3 \subset \cdots$ از زیرمدولها داده‌شده‌است . به آسانی تحقیق می‌شود که $\bigcup_{i \geq 1} A_i$ نیز زیرمدولی از A است ؛ ولذا ، با تولید متناهی ، مثلا " به وسیلهٔ $a_1, \ldots, a_k$ ، است . چون هر a_i عنصری از یک A_j است ، اندیسی مانند n وجود دارد به‌طوری‌که ، به‌ازای $i = 1,2, \ldots, k$ ، $a_i \in A_n$. درنتیجه ، $\bigcup A_i \subset A_n$ ؛ درنتیجه ، به‌ازای $i \geq n$ ، $A_i = A_n$.

این بخش را با بردن نتایج اصلی بخش II ۸ ، که درباب سری زیرنرمال برای گروهها است ، به‌مدولها خاتمه می‌دهیم . این مطالب را برای اثبات نتیجهٔ ۱۲.۱ ، که در فصل نه مفید واقع می‌شود ، ذکر می‌کنیم . بحث را با چند تعریف ، که اغلبشان با تعاریف مربوط به گروهها در بخش II ۸ یکی است ، آغاز می‌کنیم .

یک *سری نرمال* برای مدول A زنجیری است از زیرمدولها مانند

$$A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n ,$$

عاملهای سری مدولهای خارج‌قسمتی

$$A_i/A_{i+1} \quad (i = 0,1, \ldots, n-1)$$

می‌باشند . *طول* سری تعداد شمولهای حقیقی (= تعداد عوامل نابدیهی) می‌باشد . یک *تظریف* سری نرمال $A_0 \supset A_1 \supset \cdots \supset A_n$ یک سری نرمال است که از درج تعدادی متناهی زیرمدول اضافی بین زیرمدولهای داده شده به دست می‌آید . یک *تظریف حقیقی* تظریفی است که طولش از طول سری اصلی بزرگتر باشد . دو سری نرمال *معادل* هستند اگر تناظر یک به یکی بین عوامل نابدیهی موجود باشد به‌طوری‌که عوامل نظیر مدولهایی یکریخت باشند . لذا ، سریهای معادل لزوما " یک طول خواهند داشت . یک *سری ترکیبی* برای A سری نرمالی مانند $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = 0$ است به‌طوری‌که هر عامل A_k/A_{k+1} $(k = 0,1, \ldots, n-1)$ مدول ناصفری بدون زیرمدولهای حقیقی می‌باشد .[1]

---

۱ . *هرگاه R یکدار باشد ، آنگاه یک مدول یکانی ناصفر بدون زیرمدول حقیقی را ساده می‌گویند . در این حالت ، یک سری ترکیبی سری نرمال $A = A_0 \supset \cdots \supset A_n = 0$ با عوامل ساده می‌باشد . اگر R یکدار نباشد ، ساده بودن طور دیگر تعریف می‌شود . ر.ک. تعریف IX ۱۰.۱۰ و تبصره‌های بعد از آن .*

نتایج مختلف بخش II ۸.۰ را می‌توان به‌آسانی به مدولها برد. مثلا"، *سری ترکیبی تظریف حقیقی ندارد*؛ و لذا، باهرتظریف خود معادل است (ر.ک. قضایای IV ۱۰.۱۰ و II ۴.۸.۰ ولم II ۸.۸.۰). قضایای شریر، زاسن‌هاوس، و ژردان ــ هولدر برای مدولها معتبرند:

قضیهٔ ۱۰.۱. *هر دو سری نرمال مدول A تظریفهایی دارند که معادل‌اند. هر دو سری ترکیبی A معادل می‌باشند.*

برهان. ر.ک. نتایج نظیربرای‌گروهها (لم II ۹.۸.۰ و قضایای II ۱۰.۸.۰ و II ۱۱.۸.۰).

قضیهٔ ۱۱.۱. *مدول ناصفر A دارای‌سری‌ترکیبی‌است اگر و فقط‌اگر A در شرایط زنجیر افزایشی و کاهشی بر زیرمدولها صدق نماید.*

برهان. ($\Rightarrow$) فرض‌کنیم A دارای سری ترکیبی S به طول n باشد. اگر یکی از شرایط زنجیری برقرار نباشد، می‌توان زیرمدولهایی چون

$$A = A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots \supsetneq A_n \supsetneq A_{n+1}$$

یافت‌که‌یک سری نرمال T به‌طول $n+1$ را تشکیل دهند. بنابر قضیهٔ ۱۰.۱، S و T تظریفهایی دارندکه‌باهم معادلند. این‌تناقض‌است، زیرا سریهای معادل طولهای یکسان دارند. چون هر تظریف سری ترکیبی S همان طول n، همانند S، را دارد، ولی هر تظریف T لزوما" به طول دست‌کم $n+1$ است؛ بنابراین، A در هر دو شرط زنجیری صدق خواهد کرد.

($\Leftarrow$) اگر B زیرمدول ناصفری از A باشد، $S(B)$ را مجموعهٔ تمام زیرمدولهای C از B می‌گیریم به‌طوری‌که $C \neq B$. لذا، اگر B زیرمدول حقیقی نداشته باشد، $S(B) = \{0\}$. همچنین، تعریف می‌کنیم $S(0) = \{0\}$. بنابر قضیهٔ ۴.۱، به‌ازای هر B عنصر ماکزیمال B' از $S(B)$ وجود دارد. فرض‌کنیم S مجموعهٔ تمام زیرمدولهای A بوده و نگاشت $f: S \to S$ را با $f(B) = B'$ تعریف می‌کنیم. (اصل انتخاب برای انتخاب همزمان B' لازم است). بنابرقضیهٔ بازگشتی ۲.۶ و آشنایی (با $f = f_n$ به‌ازای هر n)، تابعی مانند

$\varphi : \mathbf{N} \to S$ وجود دارد به‌طوری‌که

$$\varphi(0) = A \quad \text{و} \quad \varphi(n+1) = f(\varphi(n)) = \varphi(n)' .$$

هرگاه A_i نمایش $\varphi(i)$ باشد، آنگاه، طبق ساخت، $A \supset A_1 \supset A_2 \supset \cdots$ یک زنجیر کاهشی است، که از آنجا، به‌ازای n ی و هر $i \geq n$ ، $A_i = A_n$. چون $A_{n+1} = A_n' = f(A_n)$ ، تعریف f نشان می‌دهدکه $A_{n+1} = A_n$ فقط اگر $A_n = 0 = A_{n+1}$. فرض کنیم m کوچکترین عددصحیحی باشدکه $A_m = 0$. پس $m \leq n$ و، به‌ازای هر $k < m$ ، $A_k \neq 0$. به علاوه، به‌ازای هر $k < m$ ، A_{k+1} زیرمدول ماکزیمالی از A_k است به‌طوری‌که $A_k \supsetneq A_{k+1}$. درنتیجه، بنابر قضیهٔ IV ۱۰۰۱۰ ، هر A_k/A_{k+1} ناصفر بوده و زیرمدول حقیقی ندارد. بنابراین، $A \supset A_1 \supset \cdots \supset A_m = 0$ یک سری ترکیبی برای A است.

نتیجهٔ ۱۲۰۱ . هرگاه D یک حلقهٔ بخشی باشد، آنگاه حلقهٔ $\mathrm{Mat}_n D$ مرکب از تمام ماتریسهای $n \times n$ روی D هم آرتینی و هم نوتری است.

طرح برهان. در پرتوتعریف ۲۰۱ وقضیهٔ ۱۱۰۱ ، کافی است نشان دهیم که $R = \mathrm{Mat}_n D$ سری ترکیبی از R ــ مدولهای چپ وسری ترکیبی از R ــ مدولهای راست دارد. به‌ازای هر i ، فرض کنیم $e_i \in R$ ماتریسی با 1_D درموضع (i,i) و 0 در جاهـــــای دیگر باشد. تحقیـــق کنیـــد که $Re_i = \{Ae_i \mid A \in R\}$ یک ایـــده‌آل چپ (زیرمدول) R مرکب از تمام ماتریسهایی در R است که ستون j آن به‌ازای هر $j \neq i$ صفر است. نشان دهید که Re_i یک ایده‌آل چپ نـــاصفر مینیمال است (یعنی، زیرمدول حقیقی ندارد). یک راه انجام این کار به وسیلهٔ ماتریسهای تبدیل مقدماتی است (تعریف VII ۷۰۲۰ و قضیهٔ VII ۸۰۲۰). فـــرض کنیـــم $M_0 = 0$ و، به‌ازای $i \geq 1$ ، قرار می‌دهیـــم $M_i = R(e_1 + e_2 + \cdots + e_i)$. تحقیـــق کنیـــد کـــه هـــر M_i یک ایـــده‌آل چـــپ R بوده و $M_i/M_{i-1} \cong Re_i$ ؛ درنتیجه، $R = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0$ یک ســـری ترکیبی از R ــ مدولهای چپ است. اســـتدلالی مشابه با ایده‌آلهای راست $e_iR = \{e_iA \mid A \in R\}$ نشان می‌دهد که R یک سری ترکیبی از R ــ مدولهای راست دارد.

تمرینات

۱ . (آ) حلقهٔ تمام ماتریسهای 2×2 ی $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ که در آنها a عددی صحیح بوده

و b,c گویا می‌باشند نوتری راست است ولی نوتری چپ نیست.

(ب) حلقهٔ تمام ماتریسهای 2×2 ی $\begin{pmatrix} d & r \\ 0 & s \end{pmatrix}$ که در آنها d گویا بوده و r,s حقیقی باشند آرتینی راست است ولی آرتینی چپ نیست.

۲. هرگاه I ایده‌آل ناصفری از دامنهٔ ایده‌آل اصلی R باشد، آنگاه حلقهٔ R/I هم نوتری است هم آرتینی.

۳. فرض کنید S زیرمجموعه‌ای ضربی از حلقهٔ نوتری تعویضپذیر یکدار R باشد. در این صورت، حلقهٔ $S^{-1}R$ نوتری است.

۴. فرض کنید R حلقه‌ای تعویضپذیر و یکدار باشد. هرگاه ایده‌آل I از R با تولید متناهی نباشد آنگاه یک زنجیر افزایشی حقیقی نامتناهی از ایده‌آلها مانند $J_1 \subset J_2 \subset \cdots$ وجود دارد به‌طوری که به‌ازای هر k، $J_k \subset I$. اجتماع J_k ها لازم نیست I باشد.

۵. هر نقش همریختی از یک حلقهٔ نوتری [آرتینی] چپ نوتری [آرتینی] چپ است.

۶. حلقهٔ R نوتری [آرتینی] چپ است اگر و فقط اگر $\mathrm{Mat}_n R$، به‌ازای هر $n \geq 1$، نوتری [آرتینی] چپ باشد [نابدیهی].

۷. هر دامنهٔ صحیح آرتینی یک میدان است. [**راهنمایی.** برای یافتن معکوس $a \neq 0$، زنجیر $(a) \supset (a^2) \supset (a^3) \supset \cdots$ را درنظر بگیرید.]

۲ ایده‌آلهای اول و اولیه

هدف اصلی ما مطالعهٔ ساختار ایده‌آلی بعضی از حلقه‌های تعویضپذیر است. ما خواص اساسی ایده‌آلهای اول را عرضه می‌کنیم. رادیکال یک ایده‌آل را معرفی کرده و ایده‌آلهای اولیه را تعریف می‌کنیم. بالاخره، تجزیهٔ اولیهٔ ایده‌آلها را مطرح خواهیم کرد. جز در قضیهٔ ۲۰۲، ***تمام حلقه‌ها تعویضپذیر می‌باشند.***

با چند مطلب زمینه شروع می‌کنیم که هم‌انگیزه بوده و هم منبع مثالهای آشنای مفاهیمی هستند که معرفی می‌شوند. انگیزهٔ قسمت اعظمی از این بخش از بررسی دامنه‌های ایده‌آل اصلی ناشی می‌شود. بخصوص، یک چنین دامنهٔ D یک دامنهٔ یکتایی تجزیه می‌باشد (قضیهٔ III ۷.۳۰).

خاصیت یکتایی تجزیهٔ D را می‌توان برحسب ایده‌آلها بیان کرد: هر ایده‌آل حقیقی D حاصلضربی از ایده‌آلهای ماکزیمال (درنتیجه، اول) است، که با تقریب

ترتیب به‌طور منحصر به‌فرد معین می‌شوند (تمرین III ۵.۳۰) . بنابر قضیهٔ III ۳.۴۰ ، هر ایده‌آل اول ناصفر D به شکل (p) بوده ، که در آن p اول (= تحویل‌ناپذیر) است ، و $(p)^n = (p^n)$. درنتیجه ، هر ایده‌آل حقیقی (a) از D را می‌توان (با تقریب ترتیب) به‌طور منحصر به فرد به شکل زیر نوشت :

$$(a) = (p_1^{n_1})(p_2^{n_2})\cdots(p_r^{n_r}) = (p_1^{n_1}) \cap (p_2^{n_2}) \cap \cdots \cap (p_r^{n_r}),$$

که در آن هر $n_i > 0$ و p_i ها عناصر اول متمایزی می‌باشند (تمرین III ۵.۳۰) . اما هر ایده‌آل $Q = (p^n)$ (p اول) دارای خاصیت زیر است : $ab \in Q$ و $a \notin Q$ ایجاب می‌کنند که ، به‌ازای k ای ، $b^k \in Q$ (تمرین III ۵.۳۰) . یک چنین ایده‌آل اولیه نام دارد . بحث پیشین نشان می‌دهد که هر ایده‌آل در یک دامنهٔ ایده‌آل اصلی به‌طریقی منحصر به فرد برابر با اشتراک تعدادی متناهی ایده‌آل اولیه می‌باشد . به علاوه ، رابطهٔ روشنی بین این ایده‌آلهای اولیه و ایده‌آلهای اول D وجود دارد ؛ درواقع ، هر ایده‌آل اولیهٔ $(p^n) = (p)^n$ توانی از یک ایده‌آل اول می‌باشد .

در روشی‌که هم‌اینک به اختصار ذکر شد ، دیدگاه از توجه به یکتایی تجزیهٔ عناصر به صورت حاصل‌ضربهایی از عناصر اول در D به "تجزیهٔ اولیهٔ" ایده‌آلها در دامنهٔ ایده‌آل اصلی D معطوف گشت . حال "تجزیهٔ اولیهٔ" ایده‌آلها را در حلقه‌های تعویضپذیر کلیتر (که در آنها ، مثلا" ، لازم نیست ایده‌آلها اصلی و ایده‌آلهای اولیه توانهایی از ایده‌آلهای اول باشند) بررسی می‌کنیم . بحث را با چند مطلب در باب ایده‌آلهای اول آغاز می‌نماییم .

قضیهٔ ۱.۲ . *ایده‌آل $P(\neq R)$ درحلقهٔ تعویضپذیر R اول است اگر و فقط اگر $R - P$ مجموعه‌ای ضربی باشد .*

برهان . این صرفا" بیان مجددی از قضیهٔ III ۱۵.۲ است ؛ ر.ک . تعریف III ۱.۴ .

تبصره . مجموعهٔ تمام ایده‌آلهای اول در حلقهٔ R *طیف* R نام دارد .

قضیهٔ ۲.۲ . *هرگاه S زیرمجموعه‌ای ضربی از حلقهٔ R و جدا از ایده‌آل I ی R باشد ، آنگاه ایده‌آلی مانند P وجود دارد که در مجموعهٔ تمام ایده‌آلهای R جدا از S و شامل*

I ماکزیمال است. به علاوه، هر چنین ایده‌آل P اول می‌باشد.

این قضیه مکرر در حالت $I = 0$ به کار می‌رود.

طرح برهان ۳.۲. مجموعهٔ $\mathcal{S}$ مرکب از تمام ایده‌آلهای R جدا از S و شامل I ناتهی است، زیرا $I \in \mathcal{S}$. چون $S \neq \varnothing$ (تعریف III ۱.۴۰)، هر ایده‌آل در $\mathcal{S}$ حقیقتا" مشمول R است. $\mathcal{S}$ به وسیلهٔ شمول جزئی مرتب است. بنابر لم زرن، ایده‌آلی مانند P وجود دارد که در $\mathcal{S}$ ماکزیمال است. فرض کنیم A,B ایده‌آلهایی از R باشند به‌طوری‌که $AB \subset P$. هرگاه $A \not\subset P$ و $B \not\subset P$، آنگاه ایده‌آلهای $P + A$ و $P + B$ حقیقتا" شامل P بوده؛ و لذا، S را قطع می‌کنند. درنتیجه، به‌ازای $p_i \in P,\ a \in A,\ b \in B$،

$$p_1 + a = s_1 \in S \quad \text{و} \quad p_2 + b = s_2 \in S .$$

لذا، $s_1 s_2 = p_1 p_2 + p_1 b + a p_2 + ab \in P + AB \subset P$. این تناقض است، زیرا $s_1 s_2 \in S$ و $S \cap P = \varnothing$. بنابراین، $A \subset P$ یا $B \subset P$، که از آنجا P اول می‌باشد.

قضیهٔ ۳.۲. *فرض کنیم* K *زیرحلقه‌ای از حلقهٔ تعویضپذیر* R *باشد. هرگاه* $P_1, \ldots, P_n$ *ایده‌آلهای اولی از* R *باشند به‌طوری‌که* $K \subset P_1 \cup P_2 \cup \cdots \cup P_n$، *آنگاه، به‌ازای* i ی، $K \subset P_i$.

تبصره. در حالت $n \leq 2$، برهان زیر از فرض اول بودن هر P استفاده نمی‌کند؛ این فرض برای $n > 2$ ضرورت دارد.

برهان ۳.۲. فرض کنیم به‌ازای هر i، $K \not\subset P_i$. پس کافی است فرض کنیم $n > 1$ و n مینیمال باشد؛ یعنی، به‌ازای هر i، $K \not\subset \bigcup_{j \neq i} P_j$. به‌ازای هر i، $a_i \in K - \bigcup_{j \neq i} P_j$ وجود دارد. چون $K \subset \bigcup P_i$، هر $a_i \in P_i$. عنصر $a_1 + a_2 a_3 \cdots a_n$ در K، و درنتیجه در $\bigcup P_i$، قرار دارد. بنابراین، $a_1 + a_2 a_3 \cdots a_n = b_j$، که در آن $b_j \in P_j$. هرگاه $j > 1$، آنگاه $a_1 \in P_j$، که تناقض است. هرگاه $j = 1$، آنگاه $a_2 a_3 \cdots a_n \in P_1$، که از آنجا، بنابرقضیهٔ III ۵.۲۰، به‌ازای $i > 1$ ی، $a_i \in P_1$. این نیز یک تناقض می‌باشد.

حکم ۴۰۲ . *هرگاه* R *حلقهٔ یکدار و تعویضپذیری بوده و* P *ایده‌آلی باشد که در مجموعهٔ تمام ایده‌آلهای* R *که با تولید متناهی نیستند ماکزیمال است ، آنگاه* P *اول خواهد بود .*

برهان . فرض کنیم $ab \in P$ ولی $a \notin P$ و $b \notin P$. در این صورت ، $P + (a)$ و $P + (b)$ ایده‌آلهایی هستند که حقیقتا" شامل P بوده ؛ و لذا (طبق ماکزیمالی) ، با تولید متناهی‌اند . درنتیجه ، به‌ازای $p_i, p_i' \in P$ و $r_i, r_i' \in R$ ی ، $P + (a) = (p_1 + r_1 a, \ldots, p_n + r_n a)$ و $P + (b) = (p_1' + r_1' b, \ldots, p_m' + r_m' b)$ (ر.ک. قضایای III ۵۰۲۰ و III ۶۰۲۰) . هرگاه $J = \{r \in R \mid ra \in P\}$ ، آنگاه J یک ایده‌آل است . چون $ab \in P$ ، به‌ازای هر i ، $(p_i' + r_i' b)a = p_i' a + r_i' ab \in P$ ، که‌از آنجا $P \subsetneq P + (b) \subset J$. بنابر ماکزیمالی ، J با تولید متناهی است ؛ مثلا" ، $J = (j_1, \ldots, j_k)$. هرگاه $x \in P$ ، آنگاه $x \in P + (a)$ ؛ و درنتیجه ، به‌ازای $s_i \in R$ ی ، $x = \sum_{i=1}^{n} s_i(p_i + r_i a) = \sum_{i=1}^{n} s_i p_i + \sum_{i=1}^{n} s_i r_i a$. درنتیجه ، $(\sum_i s_i r_i)a = x - \sum_i s_i p_i \in P$ ، که از آنجا $\sum_i s_i r_i \in J$. لذا ، به‌ازای $t_i \in R$ ی ، $\sum_{i=1}^{n} s_i r_i = \sum_{i=1}^{k} t_i j_i$ ، و $x = \sum_{i=1}^{n} s_i p_i + \sum_{i=1}^{k} t_i j_i a$. بنابراین ، P به وسیلهٔ

$$p_1, \ldots, p_n, j_1 a, \ldots, j_k a$$

تولید می‌شود ، که تناقض است . لذا ، $a \in P$ یا $b \in P$ و ، طبق قضیهٔ III ۱۵۰۲۰ ، P اول می‌باشد .

تعریف ۵۰۲ . فرض کنیم I ایده‌آلی در حلقهٔ تعویضپذیر R باشد . *رادیکال* (یا *هیچ رادیکال*) I ، که با $Rad\, I$ نموده می‌شود ، ایده‌آل $P \cap$ است ، که در آن اشتراک روی تمام ایده‌آلهای اول P شامل I گرفته شده است . هرگاه مجموعهٔ ایده‌آلهای اول شامل I تهی باشد ، آنگاه $Rad\, I$ مساوی R تعریف می‌شود .

چند تبصره . اگر R یکدارباشد ، بنابرقضیهٔ III ۱۸۰۲۰ ، هرایده‌آل $I (\neq R)$ مشمول ایده‌آل ماکزیمالی چون M است . چون $M \neq R$ و M لزوما" طبق قضیهٔ III ۱۹۰۲۰ اول است ، $\mathrm{Rad}\, I \neq R$. علی‌رغم ناسازگاری در اصطلاحات ، رادیکال ایده‌آل صفر گاهی *هیچ رادیکال* یا *رادیکال اول* حلقهٔ R نامیده می‌شود .

چند مثال. در هر دامنهٔ صحیح، ایده‌آل صفر اول است؛ درنتیجه، $\mathrm{Rad}\,0 = 0$. در حلقهٔ $\mathbf{Z}$ ، $\mathrm{Rad}(12) = (2) \cap (3) = (6)$ و $\mathrm{Rad}(4) = (2) = \mathrm{Rad}(32)$.

قضیهٔ ۶.۲ . *هرگاه I ایده‌آلی در حلقهٔ تعویضپذیر R باشد، آنگاه (به‌ازای $n > 0$ ی)،*

$$Rad\, I = \{r \in R \mid r^n \in I\} .$$

برهان. هرگاه $\mathrm{Rad}\,I = R$ ، آنگاه $\{r \in R \mid r^n \in I\} \subset \mathrm{Rad}\,I$. فرض کنیم $\mathrm{Rad}\,I \neq R$. هرگاه $r^n \in I$ و P ایده‌آل اولی شامل I باشد، آنگاه $r^n \in P$ که از آنجا، طبق قضیهٔ III ۱۵.۲۰ ، $r \in P$. لذا، $\{r \in R \mid r^n \in I\} \subset \mathrm{Rad}\,I$.

به عکس، هرگاه $r \in R$ و، به‌ازای هر $n > 0$ ، $r^n \notin I$ ، آنگاه

$$S = \{r^n + x \mid n \in \mathbf{N}^*; x \in I\}$$

یک مجموعهٔ ضربی‌است به‌طوری‌که $S \cap I = \varnothing$. بنابر قضیهٔ ۲.۲ ، ایده‌آل اولی مانند P جدا از S و شامل I وجود دارد. طبق ساخت، $r \notin P$ ؛ و درنتیجه، $r \notin \mathrm{Rad}\,I$. لذا، $\mathrm{Rad}\,I \subset \{r \in R \mid r^n \in I\}$ ایجاب می‌کند که $r \notin \mathrm{Rad}\,I$ ، که از آنجا $r \notin \{r \in R \mid r^n \in I\}$.

قضیهٔ ۷.۲ . *هرگاه $I, I_1, I_2, \ldots, I_n$ ایده‌آلهایی در حلقهٔ تعویضپذیر R باشند، آنگاه*

(یک) $Rad(Rad\,I) = Rad\,I$ ؛

(دو) $Rad(I_1 I_2 \cdots I_n) = Rad\left(\bigcap_{j=1}^{n} I_j\right) = \bigcap_{j=1}^{n} Rad\,I_j$ ؛

(سه) $Rad(I^m) = Rad\,I$.

طرح برهان. در هرحالت یکی از دو شرط مطلوب را ثابت می‌کنیم. (یک) هرگاه $r \in \mathrm{Rad}\,(\mathrm{Rad}\,I)$ ، آنگاه $r^n \in \mathrm{Rad}\,I$ ؛ درنتیجه، به‌ازای $n, m > 0$ ی، $r^{nm} = (r^n)^m \in I$. بنابراین، $r \in \mathrm{Rad}\,I$ و $\mathrm{Rad}(\mathrm{Rad}\,I) \subset \mathrm{Rad}\,I$. (دو) هرگاه $r \in \bigcap_j \mathrm{Rad}\,I_j$ ، آنگاه $m_1, m_2, \ldots, m_n > 0$ ی وجود دارند به‌طوری‌که، به‌ازای هر j ، $r^{m_j} \in I_j$. هرگاه $m = m_1 + m_2 + \cdots + m_n$ ، آنگاه $r^m = r^{m_1} r^{m_2} \cdots r^{m_n} \in I_1 I_2 \cdots I_n$ ، که از آنجا $I_1 \cdots I_n \subset \bigcap_j I_j$. بالاخره، چون $\bigcap_j \mathrm{Rad}\,I_j \subset \mathrm{Rad}\,(I_1 \cdots I_n)$ ، داریم

$$\mathrm{Rad}(I_1 \cdots I_n) \subset \mathrm{Rad}(\bigcap_j I_j).$$

(سه) حالت خاصی از (دو) است.

تعریف ۸.۲. ایده‌آل $Q(\neq R)$ در حلقهٔ تعویضپذیر R **اولیه** است اگر به‌ازای هر $a,b\in R$،

$$ab\in Q \Rightarrow b^n\in Q \quad \text{به‌ازای } n>0 \text{ ی}، \quad \text{و} \quad a\notin Q.$$

مثال. هر ایده‌آل اول مسلماً اولیه است. هرگاه p عدد صحیح اولی بوده و $n\geq 2$ عدد صحیح مثبتی باشد، آنگاه $(p)^n=(p^n)$ یک ایده‌آل اولیه در $\mathbf{Z}$ است که اول نیست (تمرین ۱۷). به‌طورکلی، توان P^n ایده‌آل اول P لازم نیست اولیه باشد.

مثال. اگر F میدان باشد، ایده‌آل (x,y) در $F[x,y]$ ماکزیمال (تمرین ۱۲)؛ و درنتیجه، اول (قضیهٔ III ۱۹.۲۰) است. به علاوه، $(x,y)^2=(x^2,xy,y^2)\subsetneq(x^2,y)\subsetneq(x,y)$. ایده‌آل (x^2,y) اولیه است و (x,y) تنها ایده‌آل اول (حقیقی) شامل (x^2,y) است (تمرین ۱۲). از اینرو، ایده‌آل اولیهٔ (x^2,y) توانی از یک ایده‌آل اول در $F[x,y]$ نیست.

تا آخر این بخش همهٔ حلقه‌ها یکدار هستند.

قضیهٔ ۹.۲. *هرگاه Q یک ایده‌آل اولیه در حلقهٔ تعویضپذیر R باشد، آنگاه $\operatorname{Rad}Q$ یک ایده‌آل اول است.*

برهان. فرض کنیم $ab\in\operatorname{Rad}Q$ و $a\notin\operatorname{Rad}Q$. پس به‌ازای n ی، $a^nb^n=(ab)^n\in Q$. چون $a\notin\operatorname{Rad}Q$، $a^n\notin Q$. چون Q اولیه‌است، عدد صحیحی مانند $m>0$ وجود دارد به‌طوری‌که $(b^n)^m\in Q$، که از آنجا $b\in\operatorname{Rad}Q$. بنابراین، طبق قضیهٔ III ۱۵.۲۰، $\operatorname{Rad}Q$ اول می‌باشد.

به خاطر قضیهٔ ۹.۲ اصطلاح زیر را می‌پذیریم. هرگاه Q یک ایده‌آل اولیه درحلقهٔ تعویضپذیر R باشد، آنگاه رادیکال P از Q *ایده‌آل اول مربوطهٔ* Q نام دارد. گوییم Q یک *ایده‌آل اولیهٔ متعلق به* P *اول* است یا Q *برای* P *اولیه* است یا Q، P ـ*اولیه*

می‌باشد. واضح است که به‌ازای ایده‌آل اولیهٔ Q داده‌شده، ایده‌آل اول مربوطهٔ $\mathrm{Rad}\ Q$ منحصر به فرد است. اما یک ایده‌آل اول P ممکن است اول مربوطهٔ چند ایده‌آل اولیهٔ مختلف باشد.

مثال. هرگاه p در $\mathbf{Z}$ اول‌باشد، آنگاه هرایده‌آل اولیهٔ $(p^2), (p^3), \ldots$ متعلق به ایده‌آل اول (p) می‌باشد. در حلقهٔ $\mathbf{Z}[x,y]$، ایده‌آلهایی $(x^2,y), (x^2,y^2), (x^2,y^3)$ و غیره همه ایده‌آلهای اولیه متعلق به ایده‌آل اول (x,y) می‌باشند (تمرین ۱۳).

قضیهٔ ۱۰.۲. *فرض کنیم Q و P ایده‌آلهایی در حلقهٔ تعویضپذیر R باشند. در این صورت، Q، برای P اولیه است اگر و فقط اگر*

(یک) $Q \subset P \subset \mathrm{Rad}\ Q$ و؛

(دو) هرگاه $ab \in Q$ و $a \notin Q$، *آنگاه* $b \in P$.

طرح برهان. فرض کنیم (یک) و (دو) برقرار باشند. هرگاه $ab \in Q$ و $a \notin Q$، آنگاه $b \in P \subset \mathrm{Rad}\ Q$، که از آنجا، به‌ازای $n > 0$ ی، $b^n \in Q$. بنابراین، Q اولیه است. برای آنکه نشان دهیم Q برای P اولیه‌است کافی است ثابت کنیم $P = \mathrm{Rad}\ Q$. بنابر (یک)، $P \subset \mathrm{Rad}\ Q$. اگر $b \in \mathrm{Rad}\ Q$، n را کوچکترین عدد صحیحی می‌گیریم که $b^n \in Q$. اگر $n = 1$، $b \in Q \subset P$. هرگاه $n > 1$، آنگاه $b^{n-1}b = b^n \in Q$، که بنابر مینیمالی n، $b^{n-1} \notin Q$. بنابرقسمت (دو)، $b \in P$. لذا، $b \in \mathrm{Rad}\ Q$ ایجاب می‌کند که $b \in P$، که از آنجا $\mathrm{Rad}\ Q \subset P$. عکس استلزام آسان است.

قضیهٔ ۱۱.۲. *هرگاه $Q_1, Q_2, \ldots, Q_n$ ایده‌آلهای اولیه‌ای در حلقهٔ تعویضپذیر R بوده و همه برای ایده‌آل اول P اولیه باشند، آنگاه $\bigcap_{i=1}^{n} Q_i$ نیز یک ایده‌آل اولیهٔ متعلق به P می‌باشد.*

برهان. فرض کنیم $Q = \bigcap_{i=1}^{n} Q_i$. پس، بنابر قضیهٔ ۷.۲ (دو)،

$$\mathrm{Rad}\ Q = \bigcap_{i=1}^{n} \mathrm{Rad}\ Q_i = \bigcap_{i=1}^{n} P = P.$$

بخصوص، $Q \subset P \subset \operatorname{Rad} Q$. هرگاه $ab \in Q$ و $a \notin Q$ ، آنگاه، به‌ازای i ی، $ab \in Q_i$ و $a \notin Q_i$. چون Q_i ، P ــ اولیه است، بنابر قضیهٔ ۱۰۰۲ (دو) ، $b \in P$. درنتیجه، طبق قضیهٔ ۱۰۰۲ ، Q خود P ــ اولیه می‌باشد .

تعریف ۱۲۰۲ . ایده‌آل I در حلقهٔ تعویضپذیر R دارای *تجزیهٔ اولیه* است اگر $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ ، که در آن هر Q_i اولیه است . هرگاه هیچ Q_i ی شامل $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n$ نبوده و رادیکالهای Q_i ها همه متمایز باشند ، آنگاه گوییم تجزیهٔ اولیه *تحویل یافته* (یا *غیرزاید*) است .

قضیهٔ ۱۳۰۲ . *فرض کنیم I ایده‌آلی درحلقهٔ تعویضپذیر R باشد . هرگاه I تجزیهٔ اولیه داشته باشد ، آنگاه I تجزیهٔ اولیهٔ تحویل یافته دارد .*

برهان . هرگاه $I = Q_1 \cap \cdots \cap Q_n$ (Q_i اولیه) و Q_i ی شامل

$$Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n$$

باشد ، آنگاه $I = Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n$ نیز یک تجزیهٔ اولیه دارد . با حذف Q_i زاید (و اندیسگذاری مجدد) ، خواهیم داشت $I = Q_1 \cap \cdots \cap Q_k$ ، که در آن هیچ Q_i ی شامل اشتراک سایر Q_i ها نیست . فرض کنیم $P_1, \ldots, P_r$ ایده‌آلهای اول متمایز در مجموعهٔ $\{\operatorname{Rad} Q_1, \ldots, \operatorname{Rad} Q_k\}$ باشند . همچنین ، Q_i' $(1 \le i \le r)$ اشتراک تمام Q های متعلق به P_i اول باشد. بنابر قضیهٔ ۱۱۰۲ ، هر Q_i' برای P_i اولیه است . واضح است که Q_i' شامل اشتراک سایر Q_j' هاست . بنابراین ، $I = \bigcap_{i=1}^{k} Q_i = \bigcap_{i=1}^{r} Q_i'$ ؛ درنتیجه ، I دارای تجزیهٔ اولیهٔ تحویل یافته می‌باشد .

در اینجا دوسوال واضح مطرح می‌شوند . چه ایده‌آلهایی تجزیهٔ اولیهٔ تحویل یافته دارند ؟ آیا تجزیهٔ اولیهٔ تحویل یافته منحصر به فرد است ؟ در بخش بعد ، هر دو سوال در محدودهٔ کلیتری جواب داده شده‌اند (قضایای ۵۰۳ و ۶۰۳) .

تمرینات

تذکر . R همواره یک حلقهٔ تعویضپذیر است .

۱ . فرض کنید R یک حلقهٔ آرتینی تعویضپذیر یکدار باشد .

(آ) هر ایده‌آل اول R ماکزیمال است [**راهنمایی .** قضایای III ۱۶.۲۰ و III ۲۰.۲۰ و تمرینات ۵.۱ و ۷.۱] .

(ب) R فقط تعدادی متناهی ایده‌آل اول متمایز دارد .

۲ . هرگاه R یکدار بوده و $\{P_i \mid i \in I\}$ خانواده‌ای نـاتهی از ایده‌آلهای اول R باشد که با شمول خطی مرتب شده است ، آنگاه $\bigcup_{i\in I} P_i$ و $\bigcap_{i\in I} P_i$ ایده‌آلهای اول می‌باشند .

۳ . هرگاه $P_1, P_2, \ldots, P_n$ ایده‌آلهای اولی در R بوده و I ایده‌آلی باشد که به‌ازای هر i ، $I \not\subset P_i$ ، آنگاه $r \in I$ ی وجود دارد به‌طوری‌که به‌ازای هر i ، $r \notin P_i$.

۴ . هرگاه R یکدار بوده و $M_1, \ldots, M_r$ ایده‌آلهـای ماکزیمال متمایزی در R باشند ، آنگاه نشـان دهید کـه $M_1 \cap M_2 \cap \cdots \cap M_r = M_1 M_2 \cdots M_r$. آیا این در صورت تعویض "ماکزیمال" با "اول" نیز درست است ؟

۵ . هرگاه R یکدار بـاشد ، آنـگاه مجموعهٔ تمام مقسوم‌علیه‌های صفر R اجتماعی از ایده‌آلهای اول است .

۶ . فرض کنید R یکدار باشد . ایده‌آل اول P در R یک ***ایده‌آل اول مینیمال*** ایده‌آل I نام دارد اگر $I \subset P$ و ایده‌آل اولـی چون P' موجود نباشد که $I \subset P' \subsetneq P$.

(آ) هرگاه ایده‌آل I از R مشمول ایده‌آل اول P از R باشد ، آنگاه P شامل یک ایده‌آل اول مینیمـال از I است . [**راهنمایی .** مجموعهٔ تمام ایده‌آلهای اول P' را طوری زرنی کنید که $I \subset P' \subset P$.]

(ب) هر ایده‌آل حقیقی دست‌کم یک ایده‌آل اول مینیمال دارد .

۷ . رادیکال ایده‌آل I در حلقهٔ یکدار R اشتراک تمام ایده‌آلهای اول مینیمال آن است [ر.ک. تمرین ۶] .

۸ . اگر R یکدار بوده ، I ایده‌آلی باشد ، و J ایده‌آلی با تولید متناهی باشد به‌طوری که $J \subset \operatorname{Rad} I$ ، آنگاه عدد صحیح مثبتی مانند n هست به‌طوری که $J^n \subset I$.

۹ . رادیکال ایده‌آل صفر در Z_n چیست ؟

۱۰ . هرگاه S زیرمجموعه‌ای ضربی از حلقهٔ تعویضپذیر R بوده و I ایده‌آلی از R باشد ، آنگاه ، در حلقهٔ $S^{-1}R$ ، $S^{-1}(\operatorname{Rad} I) = \operatorname{Rad}(S^{-1}I)$.

۱۱ . فرض کنید $Q\ (\neq R)$ ایده‌آلی در R باشد . در این صورت ، Q اولیه است اگـر و

فقط اگر هر مقسوم‌علیه صفر در R/Q پوچ‌توان باشد (ر.ک. تمرین III ۱۲.۱۰).

۱۲. هرگاه F میدان باشد، آنگاه

(آ) ایده‌آل (x,y) در $F[x,y]$ ماکزیمال است؛

(ب) $(x,y)^2 = (x^2,xy,y^2) \subsetneq (x^2,y) \subsetneq (x,y)$؛

(پ) ایده‌آل (x^2,y) اولیه بوده و تنها ایده‌آل اول حقیقی شامل آن (x,y) است.

۱۳. ایده‌آلهای $(x^2,y),(x^3,y^2),(x^4,y^3),\ldots,(x^i,y^j),\ldots$ در حلقهٔ $\mathbf{Z}[x,y]$ همه ایده‌آلهایی اولیه متعلق به ایده‌آل اول (x,y) می‌باشند.

۱۴. قضیهٔ ۱۱.۲ در صورت مجاز بودن اشتراکهای نامتناهی درست نیست.

[راهنمایی. $\mathbf{Z}$ را درنظر بگیرید.]

۱۵. فرض کنید $f:R \to S$ یک بروریختی از حلقه‌های تعویضپذیر یکدار باشد. اگر J ایده‌آلی از S باشد، قرار دهید $I = f^{-1}(J)$.

(آ) I در R اولیه است اگر و فقط اگر J در S اولیه باشد.

(ب) هرگاه J برای P اولیه‌باشد، آنگاه I برای ایده‌آل اول $f^{-1}(P)$ اولیه است.

۱۶. برای ایده‌آل $I = (x^2,xy,2)$ در $\mathbf{Z}[x,y]$ یک تجزیهٔ اولیهٔ تحویل یافته به دست آورید و اولهای مربوطهٔ ایده‌آلهای اولیهٔ آمده در این تجزیه را تعیین نمایید.

۱۷. (آ) هرگاه p اول بوده و $n > 1$، آنگاه (p^n) اولیه است، ولی یک ایده‌آل اول $\mathbf{Z}$ نیست.

(ب) برای ایده‌آل (12600) در $\mathbf{Z}$ یک تجزیهٔ اولیهٔ تحویل یافته به دست آورید.

۱۸. هرگاه F میدان بوده و I ایده‌آل (x^2,xy) در $F[x,y]$ باشد، آنگاه دست‌کم سه تجزیهٔ اولیهٔ تحویل یافتهٔ I وجود دارند؛ این تجزیه‌ها عبارتند از

(یک) $I = (x) \cap (x^2,y)$؛ (دو) $I = (x) \cap (x^2,x+y)$؛

(سه) $I = (x) \cap (x^2,xy,y^2)$.

۱۹. (آ) تجزیه‌های زیر در حلقهٔ $\mathbf{Z}[x]$ اولیه‌اند:

$$(4,2x,x^2) = (4,x) \cap (2,x^2);$$
$$(9,3x+3) = (3) \cap (9,x+1).$$

(ب) آیا تجزیه‌های اولیهٔ قسمت (آ) تحویل یافته‌اند؟

۳ تجزیهٔ اولیه

نتایج بخش ۲ را به‌طور طبیعی به مدولها تعمیم می‌دهیم. همچنین، برای تجزیه‌های

اولیهٔ تحویل یافته (از زیرمدولها یا ایده‌آلها) حکم یکتایی را ثابت کرده و نشان می‌دهیم هر زیرمدول [ایده‌آل] یک مدول [حلقهٔ] نوتری تجزیهٔ اولیه دارد. در سراسر این بخش ***تمام حلقه‌ها تعویضپذیر و یکدار هستند و همهٔ مدولها یکانی می‌باشند.***

تعریف ۱.۳ . فرض کنیم R حلقه‌ای تعویضپذیر ویکدار بوده و B یک R ــ مدول باشد. زیرمدول $A(\neq B)$ ***اولیه*** است مشروط بر اینکه

به‌ازای عدد صحیح مثبتی چون n ، $r^nB \subset A \Rightarrow r \in R$ ، $b \notin A$ ، و $r^n b \in A$.

مثال. حلقهٔ R را به عنوان یک R ــ مدول درنظر گرفته و فرض می‌کنیم Q ایده‌آل اولیه‌ای (و درنتیجه، زیرمدولی) از R باشد. هرگاه $rb \in Q$ ، که $r \in R$ و $b \notin Q$ ، آنگاه، به‌ازای n ی، $r^n \in Q$. چون Q ایده‌آل است، این ایجاب می‌کند که $r^n R \subset Q$. از اینرو، Q یک زیرمدول اولیهٔ مدول R است. به عکس، هر زیرمدول اولیهٔ R یک ایده‌آل اولیه است (تمرین ۱). لذا، تمام نتایج زیرمدولهای اولیه در مورد ایده‌آلهای اولیه نیز برقرارند.

قضیهٔ ۲.۳ . ***فرض کنیم R حلقه‌ای تعویضپذیر و یکدار بوده و A زیرمدول اولیه‌ای از R ــ مدول B باشد. دراین‌صورت، $Q_A = \{r \in R \mid rB \subset A\}$ یک ایده‌آل اولیه در R است.***

برهان. چون $A \neq B$ ، $1_R \notin Q_A$ ، کهازآنجا $Q_A \neq R$. هرگاه $rs \in Q_A$ و $s \notin Q_A$ ، آنگاه $sB \not\subset A$. درنتیجه، به‌ازای $b \in B$ ای، $sb \notin A$ ولی $r(sb) \in A$. چون A اولیه است، به‌ازای n ی، $r^n B \subset A$ ؛ یعنی، $r^n \in Q_A$. بنابراین، Q_A اولیه می‌باشد.

فرض کنیم R ، A ، B ، و Q_A همانند درقضیهٔ ۲.۳ باشند. بنابر قضیهٔ ۲.۹ ، $\operatorname{Rad} Q_A = P_1$ یک ایده‌آل اول است. به آسانی معلوم می‌شود که [به‌ازای $n > 0$ ی، $P_1 = \{r \in R \mid r^n B \subset A$. گوییم زیرمدول اولیهٔ A از مدول B ***متعلق به ایده‌آل اول P*** است یا یک P ــ ***زیرمدول اولیهٔ*** B است اگر

$$P = \operatorname{Rad} Q_A = \{r \in R \mid r^n B \subset A \text{ ، به‌ازای } n > 0 \text{ ی}\}.$$

این اصطلاح با اصطلاح به کار رفته در مورد ایده‌آلها سازگار است. بخصوص، هرگاه J یک ایده‌آل اولیه باشد، آنگاه $Q_J = J$.

تعریف ۳۰۳ . فرض کنیم R حلقه‌ای تعویضپذیر و یکدار بوده و B یک R ــ مدول باشد. زیرمدول C از B دارای *تجزیهٔ اولیه* است اگر $C = A_1 \cap A_2 \cap \cdots \cap A_n$ ، که در آن هر A_i یک P_i ــ زیرمدول اولیه‌ای از B به‌ازای ایده‌آل اولی چون P_i از R باشد. هرگاه هیچ A_i ی شامل $A_1 \cap \cdots \cap A_{i-1} \cap A_{i+1} \cap \cdots \cap A_n$ نبوده و ایده‌آلهای $P_1, \ldots, P_n$ همه متمایز باشند، آنگاه تجزیهٔ اولیه **تحویل یافته** نامیده می‌شود.

اصطلاحات اینجا نیز با اصطلاحات به کار رفته در مورد ایده‌آلها سازگارند. هرگاه C ، A_i ، و P_i همانند در تعریف بوده و، به‌ازای هر $j \neq i$ ، $P_j \not\subset P_i$ ، آنگاه گوییم P_i یک *ایده‌آل اول تنهای* C است. به عبارت دیگر، P_i تنهاست اگر در مجموعهٔ $\{P_1, \ldots, P_n\}$ مینیمال باشد. اگر P_i تنها نباشد، گوییم **نشانیده** است.

قضیهٔ ۴۰۳ . *فرض کنیم R حلقهٔ تعویضپذیر و یکدار بوده و B یک R ــ مدول باشد. هرگاه زیرمدول C از B تجزیهٔ اولیه داشته باشد، آنگاه C تجزیهٔ اولیهٔ تحویل یافته دارد.*

طرح برهان. برهان شبیه برهان قضیهٔ ۱۳۰۲ است. توجه کنید که هرگاه $Q_A = \{r \in R \mid rB \subset A\}$ ، آنگاه $Q_{\bigcap_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} Q_{A_i}$. لذا، هرگاه $A_1, \ldots, A_r$ همه P ــ زیرمدولهای اولیه‌ای برای ایده‌آل اول P باشند، آنگاه، طبق قضیهٔ ۱۱۰۲ ، $\bigcap_{i=1}^{r} A_i$ نیز P ــ اولیه می‌باشد.

قضیهٔ ۵۰۳ . *فرض کنیم R حلقهٔ تعویضپذیر و یکدار بوده و B یک R ــ مدول باشد. همچنین، $C (\neq B)$ زیرمدولی از B با دو تجزیهٔ اولیهٔ تحویل یافتهٔ زیر باشد:*

$$A_1 \cap A_2 \cap \cdots \cap A_k = C = A_1' \cap A_2' \cap \cdots \cap A_s',$$

که در آن A_i ، P_i ــ اولیه و A_j' ، P_j' ــ اولیه است. در این صورت، $k = s$ و (پس از ترتیب مجدد در صورت لزوم)، به‌ازای $i = 1, 2, \ldots, k$ ، $P_i = P_i'$. به علاوه، هرگاه A_i و A_i' هر دو P_i ــ اولیه بوده و P_i اول تنها باشد، آنگاه $A_i = A_i'$.

برهان. با تغییر نمادها در صورت لزوم، می‌توان فرض کرد P_1 در مجموعهٔ $\{P_1, \ldots, P_k, P_1', \ldots, P_s'\}$ ماکزیمال باشد. ابتدا نشان می‌دهیم که به‌ازای j ای، $P_1 = P_j'$. فرض کنیم، به عکس، به‌ازای $j = 1,2,\ldots,s$، $P_1 \neq P_j'$. چون P_1 ماکزیمال است، به‌ازای $j = 1,2,\ldots,s$ داریم $P_1 \not\subset P_j'$. و چون تجزیهٔ اولی تحویل یافته است، $P_1, P_2, \ldots, P_k$ متمایزند؛ درنتیجه، به‌ازای $i = 2,3,\ldots,k$، $P_1 \not\subset P_i$. بنابر عکس نقیض قضیهٔ ۳.۲، $P_1 \not\subset P_2 \cup \cdots \cup P_k \cup P_1' \cup \cdots \cup P_s'$. درنتیجه، $r \in P_1$ ی وجود دارد به‌طوری‌که $r \notin P_i' (j \geq 1)$ و $r \notin P_i (i \geq 2)$. چون A_1، P_1 ــ اولیه است، به‌ازای عدد صحیح مثبتی چون n، $r^n B \subset A_1$. فرض کنیم C^* زیرمدول $\{x \in B \mid r^n x \in C\}$ باشد. هرگاه $k = 1$، آنگاه $C = A_1$؛ و درنتیجه، $C^* = B$. حکم می‌کنیم به‌ازای $k \geq 1$، $C^* = C$ و، به‌ازای $k > 1$، $C^* = A_2 \cap \cdots \cap A_k$. حال به آسانی معلوم می‌شود که، به‌ازای $k > 1$، $A_1' \cap A_2' \cap \cdots \cap A_s' = C \subset C^*$ و $A_2 \cap \cdots \cap A_k \subset C^*$. به‌عکس، هرگاه $x \notin A_i (i \geq 2)$، آنگاه $r^n x \notin A_i$ (در غیر این صورت، $r^n \in P_i$، زیرا A_i، P_i ــ اولیه است؛ درنتیجه، $r \in P_i$ زیرا P_i اول است). درنتیجه، $r^n x \notin C$، که از آنجا $x \notin C^*$. بنابراین، به‌ازای $k > 1$، $C^* \subset A_2 \cap \cdots \cap A_k$. استدلالی مشابه نشان می‌دهد که $C^* \subset A_1' \cap A_2' \cap \cdots \cap A_s' = C$؛ درنتیجه، $C^* = C$ و $(k \geq 1)$. هرگاه $k = 1$، آنگاه، همانطورکه در بالا دیدیم، $C^* = A_2 \cap \cdots \cap A_k$ $(k > 1)$. لذا $C = C^* = B$، که با $C \neq B$ متناقض است. هرگاه $k > 1$، آنگاه

$$A_2 \cap \cdots \cap A_k = C^* = C = A_1 \cap A_2 \cap \cdots \cap A_k,$$

که از آنجا $A_2 \cap \cdots \cap A_k \subset A_1$. این نتیجه با تحویل یافته بودن تجزیهٔ اول متناقض است. لذا، این فرض که به‌ازای هر j، $P_1 \neq P_j'$ همواره به تناقض می‌انجامد. بنابراین، به‌ازای j ای، مثلاً $j = 1$، $P_1 = P_j'$.

حال برهان به استقرا بر k پیش می‌رود. هرگاه $k = 1$، آنگاه حکم می‌کنیم که s نیز مساوی 1 است. زیرا هرگاه $s > 1$، آنگاه استدلال فوق به‌ازای $P_1 = P_1'$ و تعویض نقشهای A_1, A_1' نشان می‌دهد که $B = C^* = A_2' \cap \cdots \cap A_s'$، که از آنجا، به‌ازای $j \geq 2$ ای، $A_j' = B$. لذا، تجزیهٔ دوم C تحویل یافته نیست، که یک تناقض است. بنابراین، $s = 1 = k$ و $A_1 = C = A_1'$. حال فرض کنیم $k > 1$ و قضیه برای تمام زیرمدولهایی که تجزیهٔ اولیهٔ تحویل یافته‌ای با کمتر از k جمله دارند برقرار باشد. استدلال بند قبل (به‌ازای $P_1 = P_1'$) نشان می‌دهد که به‌ازای $k > 1$، زیرمدول C^*

دو تجزیهٔ اولیهٔ تحویل یافتهٔ زیر را دارد:

$$A_2 \cap A_3 \cap \cdots \cap A_k = C^* = A_2' \cap \cdots \cap A_s'.$$

به استقرا معلوم می‌شود که $k = s$ ، و (پس از اندیسگذاری مجدد) ، به‌ازای هر i ، $P_i = P_i'$. این استقرا و برهان قسمت اول قضیه را تمام می‌کند .

فرض کنیم A_1 و A_1' هردو P_1 ــ اولیه‌بوده‌و P_1 اول تنهاباشد . برای راحتی فرض می‌کنیم $i = 1$. چون P_1 تنهاست ، به‌ازای هر $j \geq 2$ ، $r_j \in P_j - P_1$ ای وجود دارد . پس به‌ازای $j > 1$ ، $t = r_2 r_3 \cdots r_k \in P_j$ ولی $t \notin P_1$. چون A_j ، P_j ــ اولیه‌است ، به‌ازای هر $j \geq 2$ عدد صحیحی مانند n_j وجود دارد به‌طوری که $t^{n_j} B \subset A_j$. به همین نحو ، به‌ازای هر $j \geq 2$ ، m_j ای وجود دارد به‌طوری‌که $t^{m_j} B \subset A_j'$. فرض کنیم $n = \max\{n_2, \ldots, n_k, m_2, \ldots, m_k\}$. در این صورت ، به‌ازای هر $j \geq 2$ ، $t^n B \subset A_j$ و $t^n B \subset A_j'$. فرض کنیم D زیرمدول $\{x \in B \mid t^n x \in C\}$ باشد . برای اتمام برهان یکتایی ، نشان خواهیم داد که $A_1 = D = A_1'$. هرگاه $x \in A_1$ ، آنگاه

$$t^n x \in A_1 \cap A_2 \cap \cdots \cap A_k = C$$

که از آنجا $x \in D$ و $A_1 \subset D$. هرگاه $x \in D$ ، آنگاه $t^n x \in C \subset A_1$. چون A_1 ، P_1 ــ اولیه بوده و $t \notin P_1$ ، به‌ازای هر $m > 0$ داریم $t^m B \not\subset A_1$. چون A_1 اولیه است ، باید داشته باشیم $x \in A_1$ (در غیر این صورت ، $t^n x \in A_1$ و $x \notin A_1$ ایجاب می‌کنند که ، طبق تعریف ۱۰۲ ، به‌ازای q ی مثبتی ، $t^q B \subset A_1$) . از اینرو ، $D = A_1$. استدلال مشابهی نشان می‌دهد که $A_1' = D$. بنابراین ، $A_1 = A_1'$.

تا بحال با مدولهایی کار کرده‌ایم که تجزیهٔ اولیه داشته‌اند . حال جواب ناقصی به سوال زیر می‌دهیم : چه مدولهایی [ایده‌آلهایی] تجزیهٔ اولیه دارند ؟

قضیهٔ ۶.۳ . *فرض کنیم* R *حلقهٔ تعویضپذیر یکداری بوده و* B *یک* R ــ *مدول باشد که در شرط زنجیر افزایشی بر زیرمدولها صدق می‌کند . در این صورت ، هر زیرمدول* $A\ (\neq B)$ *یک تجزیهٔ اولیهٔ تحویل یافته دارد : بخصوص ، هر زیرمدول* $A\ (\neq B)$ *از مدول با تولید متناهی* B *روی حلقهٔ نوتری تعوضپذیر* R *و هر* $(\neq R)$ *ایده‌آل از* R *تجزیهٔ اولیهٔ تحویل یافته دارد .*

برهان ۶.۳ . فرض کنیم $\mathcal{S}$ مجموعهٔ تمام زیرمدولهای B باشدکه تجزیهٔ اولیه **ندارند** . واضح است کـه هیچ زیرمدول اولیه‌ای در $\mathcal{S}$ نیست . باید نشان دهیم که $\mathcal{S}$ عملا" تهی است . هرگاه $\mathcal{S}$ ناتهی باشد ، آنگاه ، بنابرقضیهٔ ۴.۱ ، $\mathcal{S}$ شامل عنصر ماکزیمال C است . چون C اولیه نیست ، $r \in R$ ی و $b \in B - C$ ای وجـود دارند بـه‌طوری که $rb \in C$ ولی ، به‌ازای هر $n > 0$ ، $r^n B \not\subset C$. فرض کنیم $B_n = \{x \in B \mid r^n x \in C\}$. در این صورت ، هر B_n زیرمدولی از B است و $B_1 \subset B_2 \subset B_3 \subset \cdots$. طبق فرض ، $k > 0$ ای وجود دارد به طوری‌که به‌ازای $i \geq k$ ، $B_i = B_k$ ، فرض کنیم D زیرمدول

$$\{x \in B \mid x = r^k y + c \text{ ، ی } y \in B, c \in C \text{ به‌ازای}\}$$

باشد . واضح است که $C \subset B_k \cap D$. به عکس ، هرگاه $x \in B_k \cap D$ ، آنگاه $x = r^k y + c$ و $r^k x \in C$ ، کـه از آنجـا $r^{2k} y = r^k (r^k y) = r^k (x - c) = r^k x - r^k c \in C$. بنـابـرایـن ، $y \in B_{2k} = B_k$. درنتیجه ، $r^k y \in C$ ؛ ولذا ، $x = r^k y + c \in C$. بنابراین ، $B_k \cap D \subset C$ ، کـه از آنجـا $B_k \cap D = C$. امـا $C \neq B_k \neq B$ و $C \neq D \neq B$ ، زیـرا $b \in B_k - C$ و $r^k B \not\subset C$. بنابرماکزیمالی C در $\mathcal{S}$ ، B_k و D بایدتجزیه‌های اولیه داشته باشند . لذا ، C تجزیهٔ اولیـه دارد ، کـه یک تنـاقض است . بنابراین ، $\mathcal{S}$ تهی است و هر زیرمدول تجزیهٔ اولیـه دارد . درنتیجه ، بنـابر قضیهٔ ۴.۳ ، هر زیرمدول دارای تجزیهٔ اولیهٔ تحویل‌یافته می‌باشد . حال آخرین‌حکم قضیه نتیجهٔ فوری قضایای ۸.۱ و ۹.۱ می‌باشد .

تمرینات

تذکر. R همواره حلقه‌ای تعویضپذیر و یکدار است مگر آنکه خلافش گفته شود .

۱ . حلقهٔ R را یک R ــ مدول درنظـر بگیرید . هرگاه Q زیـر مدول اولیه‌ای از R باشد ، آنگاه Q یک ایده‌آل اولیه است .

۲ . (آ) فرض کنید $f : B \to D$ یک‌بروریختی R ــ مدولهابوده‌و $C (\neq D)$ زیرمدولی از D باشد . C یک زیرمدول‌اولیهٔ D است اگر و فقط اگر $f^{-1}(C)$ زیرمدول اولیه‌ای از B باشد .

(ب) هرگاه C و $f^{-1}(C)$ اولیه باشند ، آنگاه هر دو متعلق به یک ایده‌آل اول P هستند .

۳ . هرگاه $A (\neq B)$ زیرمدولی‌از R ــ مدول B بوده‌و P ایده‌آلی از R باشد به‌طوری که

(یک) $r \in P$ $\Rightarrow$ $rx \in A$ و $x \notin A$ $(r \in R, x \in B)$ ؛ و

(دو) به‌ازای عدد صحیح مثبتی چون n ، $r \in P \Rightarrow r^n B \subset A$ ،

آنگاه P یک ایده‌آل اول بوده و A یک P ــ زیرمدول اولیهٔ B می‌باشد .

۴ . هرگاه A یک P ــ زیرمدول اولیهٔ R ــ مدول B بوده و نیز $rx \in A$ $(r \in R, x \in B)$، آنگاه $r \in P$ یا $x \in A$.

۵ . هرگاه A یک P ــ زیرمدول اولیهٔ R ــ مدول B بوده و C زیرمدولی از B باشد به‌طوری‌که $C \not\subset A$ ، آنگاه $\{r \in R \mid rC \subset A\}$ یک P ــ ایده‌آل اولیه است .

[**راهنمایی .** تمرین ۳ ممکن است مفید باشد .]

۶ . فرض کنید A یک P ــ زیرمدول‌اولیهٔ R ــ مدول B بوده‌و C زیرمدولی‌از B باشد به‌طوری‌که $C \not\subset A$. در این صورت ، $A \cap C$ یک P ــ زیرمدول اولیهٔ C است .

[**راهنمایی .** تمرین ۳ ممکن است مفید باشد .]

۷ . اگر B یک R ــ مدول بوده و $x \in B$ ، صفرساز x ، که با $\operatorname{ann} x$ نموده می‌شود ، عبارت است از $\{r \in R \mid rx = 0\}$. نشان دهید که $\operatorname{ann} x$ یک ایده‌آل است .

۸ . هرگاه $B \neq 0$ یک R ــ مدول بوده و P در مجموعهٔ ایده‌آلهای $\{\operatorname{ann} x \mid 0 \neq x \in B\}$ ماکزیمال باشد (ر.ک. تمرین ۷) ، آنگاه P اول می‌باشد .

۹ . فرض کنید R نوتری بوده و B یک R ــ مدول باشد . هرگاه P ایده‌آل اولی باشد به‌طوری‌که به‌ازای $x \in B$ ناصفری ، $P = \operatorname{ann} x$ (ر.ک.تمرین۷) ، آنگاه P یک *اول مربوطهٔ* B نام دارد .

(آ) هرگاه $B \neq 0$ ، آنگاه یک اول مربوطهٔ B وجود دارد . [**راهنمایی .** از تمرین ۸ استفاده کنید .]

(ب) هرگاه $B \neq 0$ و B در شرط زنجیر افزایشی بر زیرمدولها صدق کند ، آنگاه ایده‌آلهای اولی چون $P_1, \ldots, P_{r-1}$ و دنباله‌ای از زیرمدولها مانند

$$B = B_1 \supset B_2 \supset \cdots \supset B_r = 0$$

وجود دارند به‌طوری که ، به‌ازای هر $i < r$ ، $B_i/B_{i+1} \cong R/P_i$.

۱۰ . فرض کنید R و B همانند در تمرین ۹ (ب) باشند . در این صورت ، شرایط‌زیر بر $r \in R$ معادلند :

(یک) به‌ازای هر $x \in B$ عددصحیح‌مثبتی‌مانند $n(x)$ هست‌به‌طوری‌که $r^{n(x)}x = 0$ ؛

(دو) r در هر اول مربوطهٔ B قرار دارد (ر.ک. تمرینهای ۹ و ۱۵) .

۱۱ . فرض کنید R نوتری بوده، $r \in R$ ، و B یک R ــ مدول باشد. در این صورت، $rx = 0$ $(x \in B)$ ایجاب می‌کند که $x = 0$ اگر و فقط اگر r در هیچ اولیهٔ مربوطهٔ B قرار نداشته باشد (ر.ک. تمرینهای ۸ و ۹).

۱۲ . فرض کنید R نوتری بوده و B یک R ــ مدول صادق در شرط زنجیر افزایشی روی زیرمدولها باشد. در این صورت، احکام زیر معادلند:

(یک) دقیقاً" یک اول مربوطهٔ B وجود دارد (ر.ک. تمرین ۹)؛

(دو) $B \neq 0$ و، به‌ازای هر $r \in R$ ، یکی از موارد زیر درست است: یا $rx = 0$ ایجاب می‌کندکه به‌ازای هر $x \in B$ ، $x = 0$ یا به‌ازای هر $x \in B$ عدد صحیح مثبتی مانند $n(x)$ هست که $r^{n(x)}x = 0$. [ر.ک. تمرینهای ۱۰ و ۱۱ .]

۱۳ . فرض کنید R و B همانند در تمرین ۱۲ باشند. در این صورت، زیرمدول A از B اولیه است اگر و فقط اگر B/A دقیقاً" یک اول مربوطهٔ P داشته باشد، که در آن صورت A ، P ــ اولیه است (ر.ک. تمرینهای ۹ و ۱۲).

۱۴ . فرض کنید R و B همانند در تمرین ۱۲ باشند. هرگاه A $(\neq B)$ زیرمدولی از B باشد، آنگاه هر اول مربوطهٔ A یک اول مربوطهٔ B است. هر اول مربوطهٔ B یک اول مربوطهٔ A یا B/A است (ر.ک. تمرین ۹).

۱۵ . فرض کنید R و B همانند در تمرین ۱۲ باشند. در این صورت، اولهای مربوطهٔ B دقیقاً" اولهای $P_1, \ldots, P_n$ اندبه‌طوری‌که $0 = A_1 \cap \cdots \cap A_n$ یک تجزیهٔ اولیهٔ تحویل‌یافتهٔ 0 بوده و هر A_i ، P_i ــ اولیه می‌باشد. بخصوص، مجموعهٔ اولهای مربوطهٔ B متناهی است. [**راهنمایی.** ر.ک. تمرینهای ۹ ، ۱۳ ، و ۱۴ .]

۱۶ . فرض کنید S یک زیرمجموعهٔ ضربی R بوده و A یک P ــ زیرمدول اولیهٔ R ــ مدول B باشد. هرگاه $P \cap S = \varnothing$ ، آنگاه $S^{-1}A$ یک $S^{-1}P$ ــ زیرمدول اولیهٔ $S^{-1}R$ ــ مدول $S^{-1}B$ است.

۴ حلقه‌ها و مدولهای نوتری

این بخش از دو قسمت مستقل تشکیل شده است. قسمت اول عمدتاً" به مدولهای نوتری (یعنی، مدولهایی که در شرط زنجیر افزایشی صدق می‌کنند) می‌پردازد. شکل نسبتاً" قوی از قضیهٔ اشتراکی کرول را ثابت می‌کنیم. لم ناکایاما[1] و چند نتیجهٔ جالب آن را

1. Nakayama

نیز عرضه می‌کنیم. در قسمت دوم این بخش، که به قسمت اول وابسته نیست، ثابت می‌کنیم هرگاه R یک حلقهٔ نوتری تعویضپذیر و یکدار باشد، آنگاه حلقهٔ چندجمله‌ای $R[x_1, \ldots, x_n]$ و حلقهٔ سری توانی $R[[x]]$ نیز چنین‌اند. بجز چند استثنا، ***تمام حلقه‌ها تعویضپذیر و یکدار می‌باشند.***

بحث را با یادآوری اینکه حلقهٔ **تعویضپذیر** R نوتری است اگر و فقط اگر R در شرط ماکزیمال برایده‌آلها (دوطرفه) صدق کند (تعریف ۲۰۱ و قضیهٔ ۴۰۱) یا، معادلا "، اگر و فقط اگر هر ایده‌آل R با تولید متناهی باشد (قضیهٔ ۹۰۱)، شروع می‌کنیم. درواقع، فقط کافی است ایده‌آلهای اول R درنظر گرفته شوند:

حکم ۱۰۴ (آی. اس. کوهن)[1]. ***حلقهٔ تعویضپذیر و یکدار*** R ***نوتری است اگر و فقط اگر هر ایده‌آل اول*** R ***با تولید متناهی باشد.***

طرح برهان. ($\Rightarrow$) فرض کنیم $\mathcal{S}$ مجموعهٔ تمام ایده‌آلهای R باشد که با تولید متناهی نیستند. هرگاه $\mathcal{S}$ ناتهی باشد، آنگاه، با استفاده از لم زرن، عنصر ماکزیمالی چون P از $\mathcal{S}$ وجود دارد. بنابر حکم ۴۰۲، P اول است؛ و درنتیجه، طبق فرض، با تولید متناهی است. این یک تناقض است مگر آنکه $\mathcal{S} = \varnothing$. بنابراین، طبق قضیهٔ ۹۰۱، R نوتری می‌باشد.

حال مقدمات لازم برای اثبات قضیهٔ اشتراکی کرول را مهیا می‌سازیم. هرگاه B مدولی روی حلقهٔ تعویضپذیر R باشد، آنگاه به آسانی معلوم می‌شود که $I = \{r \in R \mid rb = 0 \text{ ، } b \in B\}$ یک ایده‌آل R است. ایده‌آل I ***صفرساز*** B ***در*** R نام خواهد داشت.

لم ۲۰۴. *فرض کنیم* B *یک مدول با تولید متناهی روی حلقهٔ تعویضپذیر و یکدار* R *بوده و* I *صفرساز* B *در* R *باشد. در این صورت،* B *در شرط زنجیر افزایشی [کاهشی] بر زیرمدولها صدق می‌کند اگر و فقط اگر* R/I *یک حلقهٔ نوتری [آرتینی] باشد.*

---

1. *I. S. Cohen*

طرح برهان. فرض کنیم B به وسیلهٔ $b_1, \ldots, b_n$ تولید شده باشد و B در شرط زنجیر افزایشی صدق کند. بنابر قضیهٔ IV ۵۰۱۰، $B = Rb_1 + \cdots + Rb_n$. در نتیجه، $I = I_1 \cap I_2 \cap \cdots \cap I_n$، که در آن I_j صفرساز زیرمدول Rb_j است. بنابر نتیجهٔ III ۲۷۰۲۰، یک تکریختی حلقه‌ها مانند $\theta : R/I \to R/I_1 \times \cdots \times R/I_n$ وجود دارد. به آسانی معلوم می‌شود که θ یک تکریختی R ــ مدولها نیز هست. تحقیق کنید که به‌ازای هر j، نگاشت $R/I_j \to Rb_j$ داده شده با $r + I_j \mapsto rb_j$ یک یکریختی R ــ مدولهاست. چون زیرمدول Rb_j از B لزوماً در شرط زنجیر افزایشی صدق می‌کند، R/I_j نیز چنین است. بنابراین، $R/I_1 \oplus \cdots \oplus R/I_n$، باتوجه به نتیجهٔ ۷۰۱، در شرط زنجیر افزایشی بر R ــ زیرمدولها صدق می‌کند. درنتیجه، زیرمدول آن $\operatorname{Im}\theta \cong R/I$ در شرط زنجیر افزایشی بر R ــ زیرمدولها صدق می‌کند. اما هر ایده‌آل حلقهٔ R/I یک R ــ زیرمدول R/I است. بنابراین، R/I نوتری است.

به عکس، فرض کنیم R/I نوتری باشد. تحقیق کنید که B یک R/I ــ مدول با خاصیت $(r + I)b = rb$ است و R/I ــ زیرمدولهای B درست R ــ زیرمدولها می‌باشند. درنتیجه، طبق قضیهٔ ۸۰۱، B در شرط زنجیر افزایشی صدق می‌کند.

به یاد آورید که هرگاه I ایده‌آل *دلخواهی* در حلقهٔ یکدار R بوده و B یک R ــ مدول باشد، آنگاه $IB = \left\{ \sum_{i=1}^{n} r_i b_i \mid r_i \in I;\ b_i \in B;\ n \in N^* \right\}$ زیرمدولی از B می‌باشد (تمرین IV ۳۰۱۰).

لم ۳۰۴. *فرض کنیم P ایده‌آل اولی در حلقهٔ تعویضپذیر و یکدار R باشد. هرگاه C یک P ــ زیرمدول اولیهٔ R ــ مدول نوتری A باشد، آنگاه عدد صحیح مثبتی چون m وجود دارد به‌طوری که* $P^m A \subset C$.

برهان. فرض کنیم I صفرساز A در R باشد و حلقهٔ $\bar{R} = R/I$ را درنظر می‌گیریم. هم‌مجموعهٔ $r + I \in \bar{R}$ را با $\bar{r}$ نشان می‌دهیم. واضح است که $I \subset \{r \in R \mid rA \subset C\} \subset P$، که از آنجا $\bar{P} = P/I$ یک ایده‌آل $\bar{R}$ است. A و C هریک $\bar{R}$ ــ مدول باخاصیت $\bar{r}a = ra$

$(r \in R, a \in A)$ می‌باشد. حکم می‌کنیم که C یک $\bar{R}$ ــ زیرمدول اولیهٔ A است. هرگاه $ra \in C$ که $r \in R$ و $a \in A - C$، آنگاه $ra \in C$. چون C یک R ــ زیرمدول اولیه است، به‌ازای n ی، $r^n A \subset C$، که از آنجا $\bar{r}^n A \subset C$ و C، $\bar{R}$ ــ اولیه است. چون

$$\{\bar{r} \in \bar{R} \mid \bar{r}^k A \subset C \text{، ای } k > 0 \text{ به‌ازای}\} = \{\bar{r} \in \bar{R} \mid r^k A \subset C\} = (\bar{r} \in \bar{R} \mid r \in P) = \bar{P},$$

$\bar{P}$ یک ایده‌آل اول $\bar{R}$ و C یک $\bar{P}$ ــ اولیه $\bar{R}$ ــ زیرمدول A می‌باشد (ر.ک. قضایای ۹۰۲ و ۲۰۳).

چون $\bar{R}$ طبق لـم ۲۰۴ نوتری است، $\bar{P}$ طبق قضیهٔ ۹۰۱ با تولید متناهی است. فرض کنیم $\bar{p}_1, \ldots, \bar{p}_s$ $(p_i \in P)$ مولدهای $\bar{P}$ باشند. به‌ازای هر i، n_i ی هست به‌طوری که $\bar{p}_i^{n_i} A \subset C$. هرگاه $m = n_1 + \cdots + n_s$، آنگاه از قضایای III ۲۰۱۰ (پنج) و III ۵۰۲۰ (شش) نتیجه می‌شود که $P^m A \subset C$. حال این مطلب که $P = P/I$ و $IA = 0$ ایجاب می‌کنند که $P^m A \subset C$.

قضیهٔ ۴۰۴ (قضیهٔ اشتراکی کرول). *فرض کنیم R یک حلقهٔ تعویضپذیر و یکدار بوده، I یک ایده‌آل R باشد، و A یک R ــ مدول نوتری باشد. هرگاه $B = \bigcap_{n=1}^{\infty} I^n A$، آنگاه $IB = B$.*

قضیهٔ ۴۰۴ ابتدا درحالتی ثابت شد که R یک حلقهٔ موضعی نوتری با ایده‌آل ماکزیمال I بود. برهان ما (مانند برهان اصلی) به‌تجزیهٔ اولیه بستگی دارد. با اینحال، اگر فرض کنیم R نوتری باشد، برهانهای متعددی وجود دارند که در آنها از تجزیهٔ اولیه استفاده نمی‌شود (تمرین ۲).

برهان ۴۰۴. هرگاه $IB = A$، آنگاه $A = IB \subset B$، که از آنجا $B = A = IB$. هرگاه $IB \neq A$، آنگاه، بنابر قضیهٔ ۶۰۳، IB دارای تجزیهٔ اولیهٔ زیر است:

$$IB = A_1 \cap A_2 \cap \cdots \cap A_s,$$

که در آن هر A_i یک P_i ــ زیرمدول اولیهٔ A به‌ازای ایده‌آل اولی چون P_i از R است. چون در هر حال $IB \subset B$، کافی است نشان دهیم به‌ازای هر i، $B \subset A_i$ تا نتیجه بگیریم که $B \subset IB$؛ و درنتیجه، $B = IB$.

فرض کنیم i $(1 \leq i \leq s)$ ثابت باشد. ابتدا فرض می‌کنیم $I \subset P_i$. بنابر لم

۳.۴ ، عـدد صحیحی چـون m وجود دارد بـه‌طوری کـه $P_i^m A \subset A_i$ ، کـه از آنجـا $B = \bigcap_n I^n A \subset I^m A \subset P_i^m A \subset A_i$ پس $I \not\subset P_i$. حال فرض کنیم $r \in I - P_i$ ی وجود دارد.

هرگاه $B \not\subset A_i$ ، آنگاه $b \in B - A_i$ ای وجود دارد . چون $rb \in IB \subset A_i$ ، و $b \notin A_i$ ، اولیه‌است ، به‌ازای $n > 0$ ی ، $r^n A \subset A_i$. درنتیجه ، $r \in P_i$ ، زیرا A_i یک P_i ــ‌زیرمدول اولیه می‌باشد . این با انتخاب $r \in I - P_i$ تناقض دارد . بنابراین ، $B \subset A_i$.

لم ۵.۴ (ناکایاما) . *هرگاه J ایده‌آلی در حلقهٔ تعویضپذیر و یکدار R باشد ، آنگاه شرایط زیر معادل خواهند بود :*

(یک) J مشمول هر ایده‌آل ماکزیمال R است :

(دو) به‌ازای هر $j \in J$ ، $1_R - j$ یکه است ؛

(سه) هرگاه A یک R ــ مدول با تولید متناهی باشد به‌طوری‌که $JA = A$ ، آنگاه $A = 0$ ؛

(چهار) هرگاه B زیرمدولی از R ــ مدول با تولید متناهی A باشد به‌طوری‌که $A = JA + B$ ، آنگاه $A = B$.

تبصره . لم فوق حتی وقتی R تعویض‌ناپذیر باشد درست است مشروط بر اینکه (یک) با این شرط‌که J مشمول رادیکال ژاکوبسون[1] R باشد عوض شود (تمرین IX ۱۷.۲۰) .

برهان ۵.۴ . (دو) $\Rightarrow$ (یک) هرگاه $j \in J$ و $1_R - j$ یکه نباشد ، آنگاه ایده‌آل $(1_R - j)$ خود R نیست (قضیهٔ III ۲.۳۰) ؛ ولذا ، مشمول یک ایده‌آل ماکزیمال $M \neq R$ می‌باشد (قضیهٔ III ۱۸.۲۰) . اما $1_R - j \in M$ و $j \in J \subset M$ ایجاب می‌کنند که $1_R \in M$ ، که تناقض است . بنابراین ، $1_R - j$ یکه می‌باشد .

(سه) $\Rightarrow$ (دو) چون A با تولید متناهی است ، باید مجموعهٔ مولد مینیمالی مانند $X = \{a_1, \ldots, a_n\}$ از A موجود باشد (یعنی ، هیچ زیرمجموعه‌ای حقیقی از X ، A را تولید نمی‌کند) . هرگاه $A \neq 0$ ، آنگاه ، بنابر مینیمالی ، $a_1 \neq 0$. چون $JA = A$ ، $a_1 = j_1 a_1 + j_2 a_2 + \cdots + j_n a_n$ $(j_i \in J)$ ، که از آنجا $1_R a_1 = a_1$ ؛ پس $(1_R - j_1)a_1 = 0$ اگر

---

1. Jacobson

$n = 1$ و

$$(1_R - j_1)a_1 = j_2a_2 + \cdots + j_na_n \quad \text{اگر} \quad n > 1$$

چون $1_R - j_1$ در R یکه است، $a_1 = (1_R - j_1)^{-1}(1_R - j_1)a_1$. لذا، هرگاه $n = 1$، آنگاه $a_1 = 0$ که تناقض است. هرگاه $n > 1$، آنگاه a_1 ترکیبی خطی از $a_2, \ldots, a_n$ است. درنتیجه، A، $\{a_2, \ldots, a_n\}$ را تولید می‌کند که با انتخاب X متناقض است.

(چهار) $\Rightarrow$ (سه) تحقیق کنید که مدول خارج‌قسمتی A/B چنان است که $J(A/B) = A/B$، که از آنجا، طبق (سه)، $A/B = 0$ و $A = B$.

(یک) $\Rightarrow$ (چهار) هرگاه M ایده‌آل ماکزیمالی باشد، آنگاه ایده‌آل $JR + M$ شامل M است. اما $JR + M \neq R$ (در غیر این صورت، طبق (چهار)، $R = M$). درنتیجه، بنابر ماکزیمالی، $JR + M = M$. بنابراین، $J = JR \subset M$.

حال چند کاربرد لم ناکایاما را ارائه می‌دهیم، و با نتیجه‌ای شروع می‌کنیم که نقطهٔ شروع نظریهٔ تتمیمها می‌باشد.

حکم ۶.۴. *فرض کنیم J ایده‌آلی در حلقهٔ تعویضپذیر و یکدار R باشد. در این صورت، J مشمول هر ایده‌آل ماکزیمال R است اگر و فقط اگر به‌ازای هر R ــ مدول A ی صادق در شرط زنجیر افزایشی بر زیرمدولها،* $\bigcap_{n=1}^{\infty} J^nA = 0$.

برهان. ($\Leftarrow$) هرگاه $B = \bigcap_n J^nA$، آنگاه، بنابر قضیهٔ ۴.۴، $JB = B$. چون B طبق قضیهٔ ۹.۱ با تولید متناهی است، بنابر لم ۵.۴، $B = 0$.

($\Rightarrow$) می‌توان فرض کرد $R \neq 0$. هرگاه M ایده‌آل ماکزیمالی از R باشد، آنگاه $M \neq R$ و $A = R/M$ یک R ــ مدول ناصفر است که زیرمدول حقیقی ندارد (قضیهٔ IV ۱۰.۱۰). لذا، A بداهتاً "در شرط زنجیر افزایشی صدق می‌کند"، که از آنجا، طبق فرض، $\bigcap_n J^nA = 0$. چون JA زیرمدولی از A است، یا $JA = A$ یا $JA = 0$. هرگاه $JA = A$، آنگاه، به‌ازای هر n، $J^nA = A$. درنتیجه، $\bigcap_n J^nA = A \neq 0$، که تناقض است. ازاینرو، $JA = 0$. اما $J \subset JR \subset M$ ایجاب می‌کند که $JA = J(R/M) = 0$.

نتیجهٔ ۷.۴ . *هرگاه* R *یک حلقهٔ موضعی نوتری با ایده‌آل ماکزیمال* M *باشد ، آنگاه* $\bigcap_{n=1}^{\infty} M^n = 0$.

برهان . هرگاه $J = M$ و $A = R$ ، آنگاه $J^n A = M^n$ ؛ حکم ۶.۴ را به کار برید .

حکم ۸.۴ . *هرگاه* R *یک حلقهٔ موضعی باشد ، آنگاه هر* R *ــ مدول تصویری با تولید متناهی آزاد است .*

درواقع ،نتیجهٔ بسیارقویتری منسوب به آی . کاپلانسکی [۶۳] برقرار است ؛ یعنی ، هر مدول تصویری روی یک حلقهٔ موضعی (نه لزوما " تعویضپذیر) آزاد است .

برهان ۸.۴ . هرگاه P یک R ــ مدول تصویری با تولید متناهی باشد ، آنگاه ، بنابر نتیجهٔ IV ۲.۲۰ ، یک R ــ مدول آزاد F با پایهٔ متناهی و بروریختی $\pi : F \to P$ وجوددارد . درمیان تمام R ــ مدولهای آزاد F با این خاصیت یکی با پایهٔ $\{x_1, x_2, \ldots, x_n\}$ که حداقل تعداد عنصر را داراست اختیار می‌کنیم . چون π یک بروریختی است ، $\{\pi(x_1), \ldots, \pi(x_n)\}$ لزوما " P راتولیدمی‌کند . ابتدا نشان می‌دهیم که $K = \operatorname{Ker}\pi$ مشمول MF است ، که در آن M ایده‌آل ماکزیمال منحصر به فرد R است . هرگاه $K \not\subset MF$ ، آنگاه $k \in K$ ای وجود دارد که $k \notin MF$. اما $k = r_1x_1 + r_2x_2 + \cdots + r_nx_n$ ، که در آن $r_i \in R$ ها به‌طورمنحصر به‌فرد معین می‌شوند . چون $k \notin MF$ ، r_i ی مثلا " r_1 یک عنصر M نیست . بنابر قضیهٔ III ۱۳.۴۰ ، r_1 یکه است ، که از آنجا

$$x_1 - r_1^{-1}k = -r_1^{-1}r_2x_2 - \cdots - r_1^{-1}r_nx_n .$$

درنتیجه ، چون $k \in \operatorname{Ker}\pi$ ، $\pi(x_1) = \pi(x_1 - r_1^{-1}k) = \pi\left(\sum_{i=2}^{n} -r_1^{-1}r_ix_i\right) = \sum_{i=2}^{n} -r_1r_i\pi(x_i)$.

بنابراین ، P ، $\{\pi(x_2), \ldots, \pi(x_n)\}$ را تولید می‌کند . لذا ، هرگاه F' زیرمدول آزاد F با پایهٔ $\{x_2, \ldots, x_n\}$ بوده و $\pi' : F' \to P$ تحدید π به F' باشد ، آنگاه π' یک بروریختی است . این با انتخاب F که پایه‌ای با اصلیت مینیمال دارد متناقض است . از اینرو ، $K \subset MF$.

چون $0 \to K \xrightarrow{\subseteq} F \xrightarrow{\pi} P \to 0$ کامل بوده و P تصویری است ، بنابر قضیهٔ IV ۴.۳۰ ،

$K \oplus P \cong F$. تحت این یکریختی ، به‌ازای هر $k \in K$ ، $(k,0) \mapsto k$ (ر . ک . برهان قضیهٔ IV ۱۸.۱۰) ، که از آنجا F مجموع مستقیم داخلی $F = K \oplus P'$ است ، که در آن $P' \cong P$. لذا ، هرگاه $u \in F$ ، $F = K + P' \subset MF + P'$ ، آنگاه $u = \sum_i m_i v_i + p_i$ ، که در آن $m_i \in M, v_i \in F, p_i \in P'$. درنتیجه ، در R ــ مدول F/P' ،

$$u + P' = \sum_i m_i v_i + P' = \sum_i m_i (v_i + P') \in M(F/P'),$$

که از آنجا $M(F/P') = F/P'$. چون F با تولید متناهی است ، F/P' نیز چنین است . بنابراین ، طبق لم ناکایامای ۵.۴ ، $K \cong F/P' = 0$. لذا ، $P \cong P' = F$ و P آزاد است .

این بخش را با دو قضیهٔ مشهور پایان می‌دهیم . برهانها از قسمت پیشین این فصل مستقل‌اند .

قضیهٔ ۹.۴ (قضیهٔ پایهٔ هیلبرت) . *هرگاه* R *یک حلقهٔ نوتری تعویضپذیر و یکدار باشد ، آنگاه* $R[x_1, \ldots, x_n]$ *نیز چنین است .*

برهان . کافی است نشان دهیم که $R[x]$ نوتری است . بنابر قضیهٔ ۹.۱ ، کافی است نشان دهیم هر ایده‌آل J در $R[x]$ با تولید متناهی است .

به‌ازای هر $n \geq 0$ ، I_n را مجموعهٔ تمام $r \in R$ هایی می‌گیریم که $r = 0$ یا r ضریب پیشرو یک چندجمله‌ای مانند $f \in J$ از درجهٔ n است . تحقیق کنید که هر I_n یک ایده‌آل R است . هرگاه r عنصر ناصفری از I_n بوده و $f \in J$ یک چندجمله‌ای از درجهٔ n با ضریب‌پیشرو r باشد ، آنگاه r نیز ضریب پیشرو xf است ، که یک چندجمله‌ای در J از درجهٔ $n+1$ می‌باشد . از اینرو ، $I_0 \subset I_1 \subset I_2 \subset \cdots$. چون R نوتری است ، عدد صحیحی مانند t هست به‌طوری که به‌ازای هر $n \geq t$ ، $I_n = I_t$ ؛ به علاوه ، طبق قضیهٔ ۹.۱ ، هر I_n $(n \geq 0)$ با تولید متناهی است ؛ مثلاً ، $I_n = (r_{n1}, r_{n2}, \ldots, r_{ni_n})$. به‌ازای هر r_{nj} که $0 \leq n \leq t$ و $1 \leq j \leq i_n$ ، فرض کنیم $f_{nj} \in J$ یک چندجمله‌ای از درجهٔ n با

ضریب پیشرو r_{nj} باشد. توجه کنید که $f_{0j} = r_{0j} \in R \subset R[x]$. نشان می‌دهیم که ایده‌آل J از $R[x]$ به وسیلهٔ مجموعه‌ای متناهی از چندجمله‌ایها مانند

$$X = \{ f_{nj} \mid 0 \leq n \leq t; 1 \leq j \leq i_n \}$$

تولید می‌شود.

واضح است که $(X) \subset J$. به عکس، چندجمله‌ایهای از درجهٔ 0 در J دقیقاً" عناصر I_0 اند؛ و درنتیجه، مشمول (X) می‌باشند. به استقرا عمل کرده، فرض می‌کنیم (X) شامل تمام چندجمله‌ایهای J از درجهٔ کمتر از k بوده و $g \in J$ از درجهٔ k و ضریب پیشرو $r \neq 0$ می‌باشد.

هرگاه $k \leq t$، آنگاه $r \in I_k$؛ و درنتیجه، به‌ازای $s_i \in R$ ای،

$$r = s_1 r_{k1} + s_2 r_{k2} + \cdots + s_{ik} r_{ki_k}.$$

بنابراین، چندجمله‌ای $\sum_{j=1}^{i_k} s_j f_{kj} \in (X)$ دارای ضریب‌پیشرو r ودرجهٔ k است. درنتیجه، $g - \sum s_j f_{kj}$ درجه‌ای حداکثر $k-1$ دارد. بنابه فرض استقرا، $g - \sum_j s_j f_{kj} \in (X)$، که از آنجا $g \in (X)$.

هرگاه $k \geq t$، آنگاه $r \in I_k = I_t$ و $r = \sum_{j=1}^{i_t} s_j r_{tj}$ $(s_i \in R)$. به‌علاوه، $\sum_{j=1}^{i_t} s_j x^{k-t} f_{tj} \in (X)$ دارای ضریب پیشرو r و درجهٔ k می‌باشد. لذا، طبق فرض استقرا، $g - \sum_j s_j x^{k-t} f_{tj}$ درجه‌ای حداکثر $k-1$ داشته و در (X) قرار دارد. درنتیجه، $g \in (X)$ و استقرا تمام است. بنابراین، $J = (X)$.

حکم ۱۰.۴. هرگاه R یک حلقهٔ تعویضپذیر یکدار نوتری باشد، آنگاه R[[x]] نیز چنین است.

تبصره. در برهان ازحکم ۱.۴ استفاده می‌شود. با آنکه ما این کار را انجام نمی‌دهیم، ولی تکنیک به کار رفته در اثبات قضیهٔ ۹.۴ را می‌توان در اینجا نیز، پس از تعویض ضرایب ناصفر از بالاترین درجه با ضرایب از پایین‌ترین درجه، به کار برد. با اینحال، باید احتیاط کرد که سریهای توانی که در جریان اثبات به استقرا ساخته می‌شوند تعریف شده باشند. برای این کار اصل انتخاب و صورتی از قضیهٔ بازگشتی لازم می‌باشد. (این قسمت در بسیاری از برهانهای موجود از حکم ۱۰.۴ مبهم است).

برهان ۱۰.۴. بنابرحکم ۱.۴ کافی است ثابت کنیم هر ایده‌آل اول P در $R[[x]]$ با تولید متناهی است. بروزیختی حلقه‌های $R[[x]] \to R$ را با نگاشت هر سری توانی مانند $f = \sum_{i=0}^{\infty} a_i x^i$ به روی جملهٔ ثابت این سری a_0 تعریف می‌کنیم. فرض کنیم P^* نقش ایده‌آل P تحت این نگاشت باشد. در این صورت، P^* یک ایده‌آل با تولید متناهی در R است (تمرین III . ۱۳.۲ و قضیهٔ ۹.۱)، مثلاً $P^* = (r_1, \ldots, r_n)$. به ازای هر r_i، $f_i \in P$ را با جملهٔ ثابت r_i اختیار می‌کنیم.

اگر $x \in P$ ، حکم می‌کنیم که P به وسیلهٔ $r_1, \ldots, r_n, x$ تولید شده است. ابتدا توجه می‌کنیم که اگر $f_k = r_k + \sum_{i=1}^{\infty} a_i x^i$ ، آنگاه $r_k = f_k - x\left(\sum_{j=0}^{\infty} a_{j+1} x^i\right) \in P.$.

هرگاه $g = \sum_{i=0}^{\infty} b_i x^i \in P$ ، آنگاه به ازای $s_i \in R$ ، $b_0 = s_1 r_1 + \cdots + s_n r_n$ ، در نتیجه ، $g - \sum_{i=1}^{n} s_i r_i$ دارای جملهٔ ثابت 0 است؛ یعنی، $g - \sum_i s_i r_i = x g_1$. $(g_1 \in R[[x]])$.

بنابراین، $g = \sum_i s_i r_i + x g_1$ و P به وسیلهٔ $r_1, \ldots, r_n, x$ تولید شده است.

اگر $x \notin P$ ، حکم می‌کنیم که P به وسیلهٔ $f_1, \ldots, f_n \in P$ تولید شده است. هرگاه $h = \sum_{i=0}^{\infty} c_i x^i \in P$ آنگاه به ازای $t_i \in R$ ، $c_0 = t_1 r_1 + \cdots + t_n r_n$. در نتیجه، به ازای $h^* \in R[[x]]$ ، $h - \sum_{i=1}^{n} t_i f_i = x h^*$ چون $x \notin P$ و $h - \sum_i t_i f_i \in P$ و P یک ایده‌آل اول است، داریم $h^* \in P$. به ازای هر عنصر $h \in P$ ، عناصر $t_i \in R$ و $h^* \in P$ را چنان اختیار می‌کنیم که $h = \sum_{i=1}^{m} t_i f_i + x h^*$ (اصل انتخاب). فرض کنیم $\lambda : P \to P$ نگاشت تعریف شده با رابطهٔ $h \mapsto h^*$ باشد. همچنین g عنصری از P باشد. در این صورت، بنا بر قضیهٔ بازگشتی ۲.۶ در آشنایی (با به ازای هر عدد طبیعی n ، $\lambda = f_n$) یک تابع مانند $\phi : \mathbf{N} \to P$ وجود دارد به طوری که

$$\phi(0) = g \quad \text{و} \quad \phi(k+1) = \lambda(\phi(k)) = \phi(k)^*$$

فرض کنیم $\phi(k) = h_k \in R[[x]]$ و عناصر انتخاب شدهٔ قبلی از R را با t_{ki} نشان می‌دهیم که

$$h_k = \sum_{i=1}^{n} t_{ki} f_i + x h_k^* = \sum_{i=1}^{n} t_{ki} f_i + x h_{k+1}.$$

به ازای هر i $(1 \le i \le n)$ قرار می‌دهیم $g_i = \sum_{k=0}^{\infty} t_{ki}x^k \in R[[x]]$. در این صورت،

$$g_1 f_1 + \cdots + g_n f_n = \sum_{i=1}^{n} \left(\sum_{k=0}^{\infty} t_{ki}x^k \right) f_i = \sum_{k=0}^{\infty} \left(\sum_{i=1}^{n} t_{ki} f_i \right) x^k$$
$$= \sum_{k=0}^{\infty} (h_k - x h_{k+1}) x^k.$$

در نتیجه، به ازای هر $m \ge 0$ ، ضریب x^m در $g_1 f_1 + \cdots + g_n f_n$ همان ضریب x^m در $\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k$ است. چون

$$\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k = h_0 - x^{m+1} h_{m+1} = g - x^{m+1} h_{m+1},$$

ضریب x^m در $f_1 g_1 + \cdots + f_n g_n$ دقیقاً" ضریب x^m در g است. بنابراین، $g = g_1 f_1 + g_2 f_2 + \cdots + g_n f_n$ و $f_1, \ldots, f_n$ ، P را تولید خواهند کرد.

تمرینات

۱. فرض کنید R یک حلقهٔ تعویضپذیر یکدار و I یک ایده‌آل با تولید متناهی از R باشد. همچنین، C زیر مدولی از R ـ مدول A باشد. و نیز به ازای هر $r \in I$ عدد صحیح مثبتی مانند m (وابسته به r) باشد به طوری که $r^m A \subset C$. نشان دهید که به ازای عدد صحیحی مانند n ، $I^n A \subset C$. **[راهنمایی.** ر.ک. قضایای III ۲.۱۰ (پنج) و III ۵.۲۰ (شش)**]**.

۲. این صورت از قضیهٔ اشتراکی کرول را بدون استفاده از تجزیهٔ اولیه ثابت کنید. اگر R یک حلقهٔ نوتری تعویضپذیر و یکدار، I ایده‌آلی از R ، و A یک Rـمدول با تولید متناهی باشد، و نیز $B = \bigcap^{\infty} I^n A$ ، آنگاه $IB = B$. **[راهنماییها.** فرض کنید C درمجموعهٔ S مرکب از تمام زیر مدولهای S از A که $B \cap S = IB$ ماکزیمال باشد. کافی است نشان دهید که به ازای m ی $I^m A \subset C$. بنابر تمرین ۱، کافی است نشان دهید که به ازای هر $r \in I$ (تابع r) n ی هست که $r^n A \subset C$. به ازای k قرار دهید $D_k = \{a \in A \mid r^k a \in C\}$. $D_0 \subset D_1 \subset D_2 \subset \cdots$ یک زنجیرافزایشی از Rـ زیر مدولهاست. پس n ی

هست که به‌ازای هر $k \geqslant n$ ، $D_k = D_n$. نشان دهید که $(r^nA + C) \cap B = IB$. ماکزیمالی C ایجاب می‌کند که $r^nA + C = C$ ؛ یعنی ، $r^nA \subset C$.]

۳ . فرض کنید R یک حلقهٔ موضعی نوتری با ایده‌آل ماکزیمال M باشد . هرگاه ایده‌آل M/M^2 در R/M^2 به وسیلهٔ $\{a_1 + M^2, \ldots, a_n + M^2\}$ تولید شده باشد ، آنگاه ایده‌آل M در R به وسیلهٔ $\{a_1, \ldots, a_n\}$ تولید می‌شود .

۴ . (لم ناکایاما ، صورت دوم) فرض کنید R حلقه‌ای تعویضپذیر و یکدار بوده ، J ایده‌آلی مشمول هرایده‌آل ماکزیمال R باشد ، و A یک R ــ مدول با تولید متناهی باشد . هرگاه $R/J \otimes_R A = 0$ ، آنگاه $A = 0$. [**راهنمایی .** ازدنبالهٔ کامل $0 \to J \to R \to R/J \to 0$ و یکریختی طبیعی $R \otimes_R A \cong A$ استفاده کرده ، نشان دهید که $JA = A$.]

۵ . فرض کنید R و J همانند درتمرین ۴ باشند ؛ همچنین ، A یک R ــ مدول با تولید متناهی بوده و $f : C \to A$ یک همریختی R ــ مدولها باشد . در این صورت ، f یک همریختی مانند $\bar{f} : C/JC \to A/JA$ به‌طور طبیعی القامی‌کند (نتیجهٔ IV ۸.۱۰) . نشان دهید هرگاه $\bar{f}$ یک بروریختی باشد ، آنگاه f یک بروریختی است .

۶ . (آ) فرض کنید R یک حلقهٔ تعویضپذیر و یکدار باشد . هرگاه هر ایده‌آل R را بتوان بــا زیرمجموعه‌ای متناهی یا شمارشپذیر تولید کرد ، آنگاه همین امر در مورد $R[x]$ صادق است .

(ب) مشابه قسمت (آ) را برای $R[[x]]$ بیان‌وثابت کنید (جواب در اینجا کاملا" همان نیست) .

۷ . فرض کنید R حلقهٔ تعویضپذیر و یکدار بوده و $f, g \in R[[x]]$. درجهٔ اولیهٔ f (یعنی ،کوچکترین n ی‌که $a_n \neq 0$ ، در $f = \sum_{i=0}^{\infty} a_i x^i$) را با $\operatorname{In} f$ نشان می‌دهیم .

نشان دهید که

(آ) $\operatorname{In}(f+g) \geq \min(\operatorname{In} f, \operatorname{In} g)$:

(ب) $\operatorname{In}(fg) \geq \operatorname{In} f + \operatorname{In} g$ ؛

(پ) اگر R یک دامنهٔ صحیح باشد ، $\operatorname{In}(fg) = \operatorname{In} f + \operatorname{In} g$.

۸ . فرض کنید R یک حلقهٔ نوتری تعویضپذیر و یکدار بوده و $Q_1 \cap \cdots \cap Q_n = 0$ یک تجزیهٔ اولیهٔ تحویل یافته از ایده‌آل 0 از R باشد که Q_i متعلق به ایده‌آل اول

P_i است. در این صورت، $P_1 \cup P_2 \cup \ldots \cup P_n$ مجموعهٔ مقسوم‌علیه‌های صفر در R است.

۹. فرض کنید R حلقهٔ تعویضپذیر و یکدار باشد. هرگاه هر ایده‌آل ماکزیمال R به شکل (c) باشد، که در آن $c \in R$ و $c^2 = c$، آنگاه R نوتری است.
[**راهنمایی.** نشان دهید که هر ایده‌آل اولیه ماکزیمال است؛ از حکم ۱۰.۴ استفاده کنید.]

۵ توسیعهای حلقه

در قسمت اول این بخش توسیعهای حلقه را تعریف کرده و خواص توسیعهای صحیح را عرضه می‌کنیم. قسمت آخر به بررسی روابط بین ایده‌آلهای اول در حلقه‌های R و S، که S یک توسیع حلقهٔ R است، اختصاص دارد. درسراسر این بخش، ***تمام حلقه‌ها تعویضپذیر و یکدار هستند.***

تعریف ۱۰.۵. فرض کنیم S حلقه‌ای تعویضپذیر و یکدار بوده و R زیرحلقه‌ای از S شامل 1_S باشد. در این صورت، گوییم S یک **توسیع حلقهٔ** R می‌باشد.

چند مثال. واضح است که هر توسیع میدان F از میدان K یک توسیع حلقهٔ K است. هرگاه R یک حلقهٔ تعویضپذیر و یکدار باشد، آنگاه $R[[x]]$ و $R[x_1, \ldots, x_n]$ توسیعهای حلقهٔ R می‌باشند. حلقهٔ $\mathbf{Z}$ یک توسیع زیرحلقهٔ E از اعداد صحیح زوج **نیست**، زیرا E شامل 1 نمی‌باشد.

تعریف ۲۰.۵. فرض کنیم S یک توسیع حلقهٔ R بوده و $s \in S$. هرگاه یک چندجمله‌ای تکین مانند $f(x) \in R[x]$ موجود باشد به‌طوری‌که s ریشه‌ای از f باشد (یعنی، $f(s) = 0$)، آنگاه گوییم s روی R صحیح است. اگر هر عنصر S روی R صحیح باشد، گوییم S یک **توسیع صحیح** از R می‌باشد.

ویژگی مهم تعریف ۲۰.۵ شرط تکین بودن f است.

چند مثال. هرتوسیع جبری میدان F از میدان K یک توسیع صحیح حلقه است (ر.ک.

تبصره‌های بعد از تعریف ۴۰۱۰ V). حلقهٔ R روی خودش صحیح است، زیرا $r \in R$ ریشه‌ای از $x - r \in R[x]$ می‌باشد. در توسیع $\mathbf{Z}$ به وسیلهٔ میدان حقیقی $\mathbf{R}$، $1/\sqrt{3}$ روی $\mathbf{Z}$ جبری است، زیرا ریشه‌ای از $3x^2 - 1$ می‌باشد ولی $1/\sqrt{3}$ روی $\mathbf{Z}$ صحیح نیست. با اینحال، $1/\sqrt{3}$ روی میدان گویای $\mathbf{Q}$ صحیح است، زیرا یک ریشهٔ $x^2 - 1/3$ می‌باشد.

فرض کنیم S یک توسیع حلقهٔ R بوده و X زیرمجموعه‌ای از S باشد. در این صورت، **زیرحلقهٔ تولید شده به وسیلهٔ X روی R** اشتراک تمام زیرحلقه‌های S است که شامل $R \cup X$ می‌باشند؛ این زیرحلقه را با $R[X]$ نشان می‌دهیم. نیمهٔ اول قضیهٔ ۳۰۱۰ V برای حلقه‌ها معتبر است و نشان می‌دهد که $R[X]$ از تمام عناصر $f(s_1, \ldots, s_n)$ تشکیل شده است که $n \in \mathbf{N}^*$، $f \in R[x_1, \ldots, x_n]$، و $s_i \in X$. بخصوص، به‌ازای هر $s_1, \ldots, s_t \in S$، زیرحلقهٔ تولید شده به وسیلهٔ $\{s_1, \ldots, s_t\}$ روی R، که با $R[s_1, \ldots, s_t]$ نموده می‌شود، از تمام عناصر $f(s_1, \ldots, s_t)$ تشکیل شده است که $f \in R[x_1, \ldots, x_t]$. گاهی عنصری از $R[s_1, \ldots, s_t]$ یک چندجمله‌ای از $s_1, \ldots, s_t$ نام دارد. علی‌رغم این اصطلاح، $R[s_1, \ldots, s_t]$ لازم نیست با حلقهٔ چندجمله‌ای $R[x_1, \ldots, x_t]$ یکریخت باشد (مثلاً "$f(s_1, \ldots, s_t)$" ممکن است صفر باشد حتی اگر f یک چندجمله‌ای ناصفر باشد). به آسانی معلوم می‌شود که، به‌ازای هر i $(1 < i \leq t)$، $R[s_1, \ldots, s_t] = R[s_1, \ldots, s_{i-1}][s_i]$. چون $R[s_1, \ldots, s_t]$ حلقه‌ای شامل R است، $R[s_1, \ldots, s_t]$ یک R ــ مدول به‌نحو روشن می‌باشد. به همین نحو، واضح است که هر مدول روی $R[s_1, \ldots, s_t]$ یک R ــ مدول است.

قضیهٔ ۳۰۵. *فرض کنیم S یک توسیع حلقهٔ R بوده و $s \in S$. در این صورت، شرایط زیر باهم معادلند:*

(یک) s روی R صحیح است؛

(دو) $R[s]$ یک R ــ مدول با تولید متناهی است؛

(سه) یک زیرحلقه مانند T از S شامل $1s$ و $R[s]$ وجود دارد که به‌عنوان یک R ــ مدول با تولید متناهی است؛

(چهار) یک $R[s]$ ــ زیرمدول مانند B از S هست که به عنوان یک R ــ مدول با تولید متناهی بوده و صفرساز آن در $R[s]$ صفر است.

طرح برهان. (دو) $\Rightarrow$ (یک) فرض کنیم s ریشه‌ای از چندجمله‌ای تکین $f \in R[x]$ از

درجهٔ n باشد. حکم می‌کنیم که $1_R = s^0, s, s^2, \ldots, s^{n-1}$ ، $R[s]$ را به عنوان Rـمدول تولید می‌کند. همانطور که در بالا دیدیم، هر عنصر $R[s]$ به‌ازای $g \in R[x]$ ای به شکل $g(s)$ است. بنابر الگوریتم تقسیم III ۲.۶۰ ، $g(x) = f(x)q(x) + r(x)$ ، که در آن $\deg r < \deg f$. بنابراین، در S ، $g(s) = f(s)q(s) + r(s) = 0 + r(s) = r(s)$. ازاینرو، $g(s)$ یک R ــ ترکیب خطی از $1_R, s, s^2, \ldots, s^m$ است، که در آن $m = \deg r < \deg f = n$.

(سه) $\Rightarrow$ (دو) فرض کنید $T = R[s]$.

(چهار) $\Rightarrow$ (سه) فرض کنیم B زیرحلقهٔ T باشد. چون $R \subset R[s] \subset T$ ، B یک $R[s]$ ــ مدول است که، بنابر (سه)، به عنوان R ــ مدول با تولید متناهی است. چون $1_S \in B$ ، $uB = 0$ به‌ازای هر $u \in S$ ایجاب می‌کند که $u = u1_S = 0$ ؛ یعنی، صفرساز B در $R[s]$ مساوی 0 است.

(یک) $\Rightarrow$ (چهار) فرض کنیم B روی R به وسیلهٔ $b_1, \ldots, b_n$ تولید شده باشد. چون B یک $R[s]$ ــ مدول است، به‌ازای هر i ، $sb_i \in B$. بنابراین، $r_{ij} \in R$ هایی وجود دارند به‌طوری که

$$\begin{aligned} sb_1 &= r_{11}b_1 + r_{12}b_2 + \cdots + r_{1n}b_n \\ sb_2 &= r_{21}b_1 + r_{22}b_2 + \cdots + r_{2n}b_n \\ &\vdots \qquad\qquad\qquad \vdots \\ sb_n &= r_{n1}b_1 + r_{n2}b_2 + \cdots + r_{nn}b_n. \end{aligned}$$

درنتیجه،

$$\begin{aligned} (r_{11} - s)b_1 + r_{12}b_2 + \cdots + r_{1n}b_n &= 0 \\ r_{21}b_1 + (r_{22} - s)b_2 + \cdots + r_{2n}b_n &= 0 \\ &\vdots \\ r_{n1}b_1 + r_{n2}b_2 + \cdots + (r_{nn} - s)b_n &= 0. \end{aligned}$$

فرض کنیم M ماتریس $n \times n$ ، (r_{ij}) بوده و $d \in R[s]$ دترمینان ماتریس $M - sI_n$ باشد. بنابر تمرین VII ۸.۳۰ ، به‌ازای هر i ، $db_i = 0$. چون B به وسیلهٔ b_i ها تولید می‌شود، $dB = 0$. چون صفرساز B در $R[s]$ صفراست، بنابر (چهار) باید داشته باشیم $d = 0$. هرگاه f چندجمله‌ای $|M - xI_n|$ در $R[x]$ باشد، آنگاه یکی از $f, -f$ تکین بوده و

$$\pm f(s) = \pm|M - sI_n| = \pm d = 0.$$

بنابراین، s روی R صحیح می‌باشد.

نتیجهٔ ۴۰۵ . *هرگاه S یک توسیع حلقهٔ R بوده و S به عنوان یک R ــ مدول با تولید متناهی باشد ، آنگاه S یک توسیع صحیح R است .*

برهان . به‌ازای هر $s \in S$ ، در قسمت (سه) قضیهٔ ۳۰۵ قرار می‌دهیم $S = T$. پس طبق قضیهٔ ۳۰۵ (یک) ، s روی R صحیح می‌باشد .

برهان احکام بعدی به‌مطلب زیر وابسته است . هرگاه $R \subset S \subset T$ حلقه (با $1_T \in R$) باشند به‌طوری‌که T یک S ــ مدول با تولید متناهی و S یک R ــ مدول با تولید متناهی باشد ، آنگاه T یک R ــ مدول با تولید متناهی می‌باشد . بند دوم برهان قضیهٔ IV ۱۶۰۲۰ نعل به نعل شامل برهانی از این امر می‌باشد .

قضیهٔ ۵۰۵ . *هرگاه S یک‌توسیع حلقهٔ R بوده و $s_1, \ldots, s_t \in S$ روی R صحیح باشند ، آنگاه $R[s_1, \ldots, s_t]$ یک R ــ مدول با تولید متناهی و یک‌توسیع صحیح حلقهٔ R می‌باشد .*

برهان . ما زنجیر

$$R \subset R[s_1] \subset R[s_1, s_2] \subset \cdots \subset R[s_1, \ldots, s_t]$$

از توسیعهای حلقه را داریم . به‌ازای هر i ، s_i روی R ، و درنتیجه روی $R[s_1, \ldots, s_{i-1}]$ ، $R[s_1, \ldots, s_{i-1}][s_i]$ صحیح است . چون $R[s_1, \ldots, s_i] = R[s_1, \ldots, s_{i-1}][s_i]$ ، بنابر قضیهٔ ۳۰۵ (یک) و (دو) روی $R[s_1, \ldots, s_{i-1}]$ یک مدول با تولید متناهی است . کاربرد مکرر تبصره‌های پیش از قضیه نشان می‌دهد که $R[s_1, \ldots, s_n]$ یک R ــ مدول با تولید متناهی است . لذا ، طبق نتیجهٔ ۴۰۵ ، $R[s_1, \ldots, s_n]$ یک توسیع صحیح از حلقهٔ R می‌باشد .

قضیهٔ ۶۰۵ . *هرگاه T یک توسیع صحیح از حلقهٔ S و S یک توسیع صحیح از حلقهٔ R باشد ، آنگاه T یک توسیع صحیح از حلقهٔ R می‌باشد .*

برهان . T بوضوح یک توسیع حلقهٔ R است . هرگاه $t \in T$ ، آنگاه t روی S صحیح بوده ؛ ولذا ، ریشهٔ چندجمله‌ای تکینی مانند $f \in S[x]$ ، مثلاً " $f = \sum_{i=0}^{n} s_i x^i$ ، می‌باشد . چون f

نیز یک چندجمله‌ای روی حلقهٔ $R[s_0, s_1, \ldots, s_{n-1}]$ است ، t روی $R[s_0, \ldots, s_{n-1}]$ صحیح می‌باشد . بنابرقضیهٔ ۳۰۵ ، $R[s_0, \ldots, s_{n-1}][t]$ ، $R[s_0, \ldots, s_{n-1}]$ ــ مدول با تولید متناهی است . اما ،چون S روی R صحیح است ، بنابر قضیهٔ ۵۰۵ ، $R[s_0, \ldots, s_{n-1}]$ ، R ــ مدول با تولید متناهی است . تبصره‌های پیش از قضیهٔ ۵۰۵ نشان می‌دهد که

$$R[s_0, \ldots, s_{n-1}][t] = R[s_0, \ldots, s_{n-1}, t]$$

یک R ــ مدول با تولید متناهی است . چون $R[t] \subset R[s_0, \ldots, s_{n-1}, t]$ ، بنابر قضیهٔ ۳۰۵ (سه) ، t روی R صحیح است .

قضیهٔ ۷۰۵ . *فرض کنیم S یک توسیع حلقهٔ R بوده و $\hat{R}$ مجموعهٔ تمام عناصر از S باشد که روی R صحیح‌اند . در این صورت ، $\hat{R}$ یک توسیع صحیح از حلقهٔ R است که شامل هر زیرحلقهٔ S که روی R صحیح است ، می‌باشد .*

برهان . هرگاه $s, t \in \hat{R}$ ، آنگاه $s, t \in R[s, t]$ ، که از آنجا $t - s \in R[s, t]$ و $ts \in R[s, t]$. چون s و t روی R صحیح‌اند ، حلقهٔ $R[s, t]$ نیز چنین است (قضیهٔ ۵۰۵) . بنابراین $t - s \in \hat{R}$ و $ts \in \hat{R}$. درنتیجه ، $\hat{R}$ زیرحلقهٔ S می‌باشد (ر.ک. قضیهٔ ۵۰۲۰۱) . $\hat{R}$ شامل R است ، زیرا هر عنصر R بداهتا " روی R صحیح است . تعریف $\hat{R}$ تضمین می‌کند که $\hat{R}$ روی R صحیح بوده و شامل تمام زیرحلقه‌های S که روی R صحیح‌اند می‌باشد .

هرگاه S یک توسیع حلقهٔ R باشد ، آنگاه حلقهٔ $\hat{R}$ از قضیهٔ ۷۰۵ **بست صحیح** R در S نام دارد . هرگاه $\hat{R} = R$ ، آنگاه گوییم R در S **به‌طور صحیح بسته** است .

چند تبصره . (یک) چون $1_R \in R \subset \hat{R}$ ، S یک توسیع حلقهٔ $\hat{R}$ است . قضایای ۶۰۵ و ۷۰۵ ایجاب می‌کنند که خود $\hat{R}$ در S به‌طور صحیح بسته باشد . (دو) مفاهیم بست صحیح و حلقه‌های بسته‌طور صحیح بسته مفاهیمی نسبی هستند و در رابطه با حلقهٔ معلوم R و توسیع حلقهٔ خاص S می‌باشند . لذا ، عبارت " R به‌طور صحیح بسته است " مبهم است مگرآنکه یک‌توسیع حلقهٔ S مشخص شده باشد . اما یک حالت وجود دارد که در آن حلقهٔ S بدون ذکر صریح مشخص است . گوییم دامنهٔ صحیح R **به‌طورصحیح بسته** است مشروط بر اینکه R در میدان خارج قسمتی آن به‌طور صحیح بسته باشد (ر.ک. ص ۲۲۴) .

مثال. دامنهٔ صحیح $\mathbf{Z}$ به‌طور صحیح بسته است (در میدان گویای $\mathbf{Q}$؛ تمرین ۸). در هر حال، $\mathbf{Z}$ در میدان اعداد مختلط $\mathbf{C}$ به‌طور صحیح بسته نیست. زیرا $i \in \mathbf{C}$ روی $\mathbf{Z}$ صحیح است.

مثال. درحالت کلی، هر دامنهٔ یکتایی تجزیه به‌طور صحیح بسته است (تمرین ۸). بخصوص، حلقهٔ چندجمله‌ای $F[x_1, \ldots, x_n]$ (F یک میدان) در میدان خارج‌قسمتی $F(x_1, \ldots, x_n)$ خود به‌طور صحیح بسته است.

قضیهٔ زیر فقط در برهان قضیهٔ ۱۰.۶ به کار می‌رود.

قضیهٔ ۸.۵. *فرض کنیم T یک زیرمجموعهٔ ضربی از دامنهٔ صحیح R باشد به‌طوری‌که $0 \notin T$. هرگاه R به‌طور صحیح بسته باشد، آنگاه $T^{-1}R$ یک دامنهٔ صحیح به‌طور صحیح بسته است.*

طرح برهان. $T^{-1}R$ یک دامنهٔ صحیح است (قضیهٔ III ۳.۴۰ (دو)) و R را می‌توان با زیرحلقه‌ای از $T^{-1}R$ یکی کرد (قضیهٔ III ۴.۴۰ (دو)). با توسیع این انطباق، می‌توان میدان خارج‌قسمتی $Q(R)$ از R را زیرمیدانی از میدان خارج‌قسمتی $Q(T^{-1}R)$ از $T^{-1}R$ درنظر گرفت. تحقیق کنید که $Q(R) = Q(T^{-1}R)$.

فرض کنیم $u \in Q(T^{-1}R)$ روی $T^{-1}R$ صحیح باشد؛ پس به‌ازای $r_i \in R$ هایی و $s_i \in T$ هایی،

$$u^n + (r_{n-1}/s_{n-1})u^{n-1} + \cdots + (r_1/s_1)u + (r_0/s_0) = 0.$$

این معادله را در s^n ضرب می‌کنیم، که $s = s_0 s_1 \cdots s_{n-1} \in T$، و نتیجه می‌گیریم که su روی R صحیح است. چون $su \in Q(T^{-1}R) = Q(R)$ و R به‌طور صحیح بسته است، داریم $su \in R$. بنابراین، $u = su/s \in T^{-1}R$، که از آنجا $T^{-1}R$ به‌طور صحیح بسته می‌باشد.

تا پایان این بخش به کشف روابط بین ایده‌آلهای (اول) در حلقه‌های R و S اختصاص دارد، که S یک توسیع حلقهٔ R می‌باشد. تنها جایی در آینده که این مطلب به کار می‌رود برهان لم ۳.۷ است.

اگر S یک توسیع حلقهٔ R بوده و $I (\neq S)$ ایده‌آلی از S باشد، به آسانی معلوم

می‌شود که $I \cap R \neq R$ و $I \cap R$ ایده‌آلی از R است (تمرین ۱۰). ایده‌آل $J = I \cap R$ **انقباض** I به R نام دارد و می‌گوییم I **روی** J **قرار دارد**.

هرگاه Q ایده‌آل اولی در توسیع حلقهٔ S از حلقهٔ R باشد، آنگاه انقباض $Q \cap R$ از Q به R یک ایده‌آل اول R می‌باشد (تمرین ۱۰). عکس مسئله چنین است: به‌ازای ایده‌آل اول P در R، آیا ایده‌آل اولی چون Q در S که روی P قرار داشته باشد (یعنی، $Q \cap R = P$) وجوددارد؟ مثالهای زیادی وجود دارند که در آنها جواب منفی است (مثلا "، توسیع $\mathbf{Z}$ به وسیلهٔ میدان اعداد گویای $\mathbf{Q}$). جواب جزئی مسئله در قضیهٔ زیر داده شده است، که به کوهن ــ زیدنبرگ[1] منسوب است.

قضیهٔ ۹.۵ (قضیهٔ رو قرار داشتن). *فرض کنیم S یک توسیع صحیح از حلقهٔ R بوده و P یک ایده‌آل اول R باشد. در این صورت، ایده‌آل اولی چون Q در S موجود است که روی P قرار دارد (یعنی، $Q \cap R = P$).*

برهان. چون P اول است، پس $R - P$ یک زیرمجموعهٔ ضربی R (قضیهٔ ۱۰.۲)، و درنتیجه زیرمجموعه‌ای ضربی از S، است. واضح است که $0 \notin R - P$. بنابر قضیهٔ ۲۰.۲، یک ایده‌آل مانند Q از S وجود دارد که در مجموعهٔ تمام ایده‌آلهای I از S که $I \cap (R - P) = \varnothing$ ماکزیمال است؛ به علاوه، هر چنین ایده‌آل Q در S اول است. واضح است که $Q \cap R \subset P$. اگر $Q \cap R \neq P$، $u \in P$ را طوری می‌گیریم که $u \notin Q$. در این صورت، ایده‌آل $Q + (u)$ در S حقیقتا "شامل Q است. بنابر ماکزیمالی، عنصری مانند $c \in (Q + (u)) \cap (R - P)$ وجود دارد؛ مثلا "، $(q \in Q; s \in S)\ c = q + su$. چون s روی R صحیح است، $r_i \in R$ ی وجود دارد به‌طوری که

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0.$$

با ضرب این معادله در u^n، نتیجه می‌شود که

$$(su)^n + r_{n-1}u(su)^{n-1} + \cdots + r_1 u^{n-1}(su) + r_0 u^n = 0.$$

چون $su = c - q$، قضیهٔ دو جمله‌ای III ۶.۱۰ ایجاب می‌کند که

$$v = c^n + r_{n-1}uc^{n-1} + \cdots + r_1 u^{n-1}c + r_0 u^n \in Q.$$

---

1. Seidenberg

اما $v \in R$ ؛ و درنتیجه، $v \in R \cap Q \subset P$. اما $u \in P$ و $v \in P$ ایجاب می‌کنندکه $c^n \in P$. چون P اول است، c باید در P قرار داشته باشد، که یک تناقض است.

نتیجهٔ ۱۰.۵ (قضیهٔ بالا رفتن). *فرض کنیم S یک‌توسیع صحیح از حلقهٔ R بوده و P_1 و P ایده‌آلهای اولی در R باشند به‌طوری‌که $P_1 \subset P$. هرگاه Q_1 ایده‌آل اولی از S باشد که روی P_1 قرار دارد، آنگاه ایده‌آل اولی چون Q از S هست به‌طوری که $Q_1 \subset Q$ و Q روی P قرار دارد.*

طرح برهان. همانند در برهان قضیهٔ ۹.۵ ، $R - P$ یک مجموعهٔ ضربی در S است. چون $Q_1 \cap R = P_1 \subset P$ ، داریم $Q_1 \cap (R - P) = \varnothing$. طبق قضیهٔ ۲.۲ ، ایده‌آل اولی چون Q از S وجود دارد که شامل Q_1 بوده و در مجموعهٔ تمام ایده‌آلهای I از S که $Q_1 \subset I$ و $I \cap (R - P) = \varnothing$ ماکزیمال است. حال می‌توان با استفاده از برهان قضیهٔ ۹.۵ نشان داد که $Q \cap R = P$.

قضیهٔ ۱۱.۵ . *فرض کنیم S یک توسیع صحیح از حلقهٔ R و P یک ایده‌آل اول در R باشد. هرگاه Q و Q' ایده‌آلهای اولی در S باشند به‌طوری که $Q \subset Q'$ و هر دوی Q و Q' روی P قرار داشته باشند، آنگاه $Q = Q'$.*

برهان. کافی است حکم زیر را ثابت کنیم : هرگاه Q ایده‌آل اولی در S باشد به‌طوری که $Q \cap R = P$ ، آنگاه Q درمجموعهٔ S مرکب از تمام ایده‌آلهای I در S با خاصیت $I \cap (R - P) = \varnothing$ ماکزیمال است.

هرگاه Q در S ماکزیمال نباشد، آنگاه ایده‌آلی چون I در S هست که

$$Q \subsetneq I \quad \text{و} \quad I \cap (R - P) = \varnothing .$$

درنتیجه، $I \cap R \subset P$. عنصر $u \in I - Q$ را اختیار می‌کنیم. چون u روی R صحیح است، مجموعهٔ تمام چندجمله‌ایهای تکین $f \in R[x]$ که $\deg f \geq 1$ و $f(u) \in Q$ ناتهی است.

از این f ها یکی باکوچکترین درجه، مثلا $f = \sum_{i=0}^{n} r_i x_i$ ، را اختیار می‌کنیم. در این‌صورت،

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u + r_0 \in Q \subset I,$$

که از آنجا $r_0 \in I \cap R \subset P = Q \cap R \subset Q$. بنابراین ،

$$u(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_2u + r_1) \in Q.$$

بنابر مینیمالی $\deg f$ ، $(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_1) \notin Q$ ، و بنابر انتخاب ، $u \notin Q$ ، این یک تناقض است ، زیرا Q اول است (قضیهٔ III ۱۵۰۲۰) . بنابراین ، Q در S ماکزیمال می‌باشد .

قضیهٔ ۱۲۰۵ . *فرض کنیم S یک توسیع صحیح از حلقهٔ R بوده و Q یک ایده‌آل اول در S باشد که روی ایده‌آل اول P در R قرار دارد . Q در S ماکزیمال است اگر و فقط اگر P در R ماکزیمال باشد .*

برهان . فرض کنیم Q در S ماکزیمال باشد . بنابر قضیهٔ III ۱۸۰۲۰ ، یک ایده‌آل ماکزیمال مانند M از R وجود دارد که شامل P است . بنابر قضیهٔ III ۹۰۲۰ ، M اول است . و طبق نتیجهٔ ۱۰۰۵ ، ایده‌آل اولی چون Q' در S هست به‌طوری که $Q \subset Q'$ و Q' روی M قرار دارد . چون Q' اول است ، $Q' \neq S$ (تعریف III ۱۴۰۲۰) . ماکزیمالی Q ایجاب می‌کند که $Q = Q'$ ، که از آنجا $P = Q \cap R = Q' \cap R = M$. بنابراین ، P در R ماکزیمال است .

به عکس ، فرض کنیم P در R ماکزیمال باشد . چون Q در S اول است ، $Q \neq S$ و یک ایده‌آل ماکزیمال مانند N از S شامل Q وجود دارد (قضیهٔ III ۱۸۰۲۰) . بنابر قضیهٔ III ۱۹۰۲۰ ، N اول است ، که از آنجا $1_R = 1_S \notin N$. چون

$$P = R \cap Q \subset R \cap N \subsetneq R$$

بنابر ماکزیمالی باید داشته‌باشیم $P = R \cap N$. لذا ، Q و N هر دو روی P قرار دارند و $Q \subset N$. بنابراین ، طبق قضیهٔ ۱۱۰۵ ، $Q = N$.

تمرینات

تذکر . S همواره یک توسیع حلقهٔ R است مگر خلافش تصریح شود .

۱ . فرض کنید S یک توسیع صحیح از حلقهٔ R بوده‌و R و S دامنه‌های‌صحیحی‌باشند. S میدان‌است‌اگرو فقط‌اگر R میدان‌باشد . [**راهنمایی .** نتیجهٔ III ۲۱۰۲۰.]

۲ . فرض کنید R یک دامنهٔ صحیح باشد . هرگاه میدان خارج‌قسمتی F از R روی R

صحیح باشد، آنگاه R میدان است.

۳. فرض کنید R دامنهٔ صحیحی با میدان خارج‌قسمتی F باشد. هرگاه $a \in R$ و $0 \neq a \in R$ و $1_R/a \in F$ روی R صحیح باشد، آنگاه a یک یکه در R است.

۴. (آ) فرض کنید R یک دامنهٔ صحیح با میدان خارج‌قسمتی F باشد. هرگاه $0 \neq a \in R$، آنگاه احکام زیر باهم معادلند:

(یک) هر ایده‌آل اول ناصفر R شامل a است؛

(دو) هر ایده‌آل ناصفر R شامل توانی از a است؛

(سه) $F = R[1_R/a]$ (توسیع حلقه).

دامنهٔ صحیح R که شامل عنصر $0 \neq a$ ی صادق در (یک) تا (سه) باشد یک **حلقهٔ گولدمن**[1] نام دارد.

(ب) یک دامنهٔ ایده‌آل اصلی حلقهٔ گولدمن است اگر و فقط اگر فقط تعدادی متناهی اول متمایز داشته باشد.

(پ) آیا نقش همریخت یک حلقهٔ گولدمن نیز حلقهٔ گولدمن است؟

۵. هرگاه S یک‌توسیع صحیح ازحلقهٔ R بوده‌و $f: S \to S$ یک همریختی حلقه‌ها باشد به‌طوری‌که $f(1_S) = 1_S$، آنگاه $f(S)$ یک توسیع صحیح از حلقهٔ $f(R)$ می‌باشد.

۶. هرگاه S یک توسیع صحیح از حلقهٔ R باشد، آنگاه $S[x_1, \ldots, x_n]$ یک توسیع صحیح از حلقهٔ $R[x_1, \ldots, x_n]$ می‌باشد.

۷. اگر S یک توسیع صحیح از حلقهٔ R بوده و T یک زیرمجموعهٔ ضربی R باشد $(0 \notin T)$، آنگاه $T^{-1}S$ توسیع صحیح $T^{-1}R$ می‌باشد. [**راهنمایی.** هرگاه $s/t \in T^{-1}S$، آنگاه $s/t = \phi_T(s)(1_R/t)$، که در آن $\phi_T: S \to T^{-1}S$ نگاشت کانونی است (قضیهٔ III ۴.۴۰). نشان دهید که $\phi_T(s)$ و $1_R/t$ روی $T^{-1}R$ صحیح‌اند، که از آنجا، بنابر قضیهٔ ۵.۵، s/t روی $T^{-1}R$ صحیح می‌باشد.]

۸. هر دامنهٔ یکتایی تجزیه به‌طور صحیح بسته است. [**راهنمایی.** حکم III ۸.۶۰.]

۹. فرض کنید T حلقهٔ تعویضپذیر و یکداری بوده و $\{S_i \mid i \in I\}, \{R_i \mid i \in I\}$ خانواده‌هایی از زیرحلقه‌ها باشند به‌طوری‌که T یک توسیع حلقهٔ S_i بوده و S_i یک توسیع حلقهٔ R_i به‌ازای هر i باشد. هرگاه هر R_i در S_i به‌طور صحیح بسته باشد، آنگاه $\bigcap_i R_i$ در $\bigcap_i S_i$ به‌طور صحیح بسته است.

---

1. Goldmann

۱۰ . (آ) هرگاه $I (\neq S)$ ایده‌آلی از S باشد، آنگاه $R \neq I \cap R$ و $I \cap R$ ایده‌آلی از R است.

(ب) هرگاه Q ایده‌آل‌اولی‌از S باشد، آنگاه $Q \cap R$ ایده‌آل‌اولی از R می‌باشد.

۶ دامنه‌های دد کیند

در این بخش رده‌ٔ دامنه‌های دد کیند را بررسی می‌کنیم. این رده حقیقتا" بین رده‌ٔ دامنه‌های ایده‌آل اصلی و رده‌ٔ دامنه‌های صحیح نوتری قرار دارد. دامنه‌های دد کیند در نظریه‌ٔجبری اعدادو نظریه‌ٔجبری منحنیهامهمند. نتیجه‌ٔ اصلی قضیه‌ٔ ۱۰.۶ است، که دامنه‌های دد کیند را به طرق مختلف توصیف می‌نماید.

نکات زیر انگیزه‌ٔ تعریف دامنه‌ٔ دد کیند که ذیلا" داده می‌شود می‌باشند. هر دامنه‌ٔ ایده‌آل اصلی D نوتری است (لم III ۶.۳۰). درنتیجه، هر ایده‌آل $(\neq D)$ دارای‌تجزیه‌ٔاولیه‌می‌باشد (قضیه‌ٔ ۶.۳). مقدمه‌ٔبخش ۲ نشان می‌دهد که در یک دامنه‌ٔ ایده‌آل اصلی شکل نسبتا" خاصی ازتجزیه‌ٔاولیه برقرار است؛ یعنی، هر ایده‌آل حقیقی حاصل‌ضربی (منحصر به فرد) از ایده‌آلهای اول است.

تعریف ۱۰۶ . هر ***دامنهٔ دد کیند*** یک‌دامنه‌ٔ صحیح مانند R است‌که‌در آن هر ایده‌آل $(\neq R)$ حاصل‌ضرب تعدادی متناهی ایده‌آل اول می‌باشد.

مثال . بحث پیش نشان می‌دهد که هر دامنه‌ٔ ایده‌آل اصلی دد کیند است. اما عکس این درست نیست. بعد از قضیه‌ٔ ۱۰.۶ در زیر مثالی از دامنه‌ٔ دد کیند آمده است که یک دامنه‌ٔ ایده‌آل اصلی نیست.

از تعریف روشن نیست که هر دامنه‌ٔ دد کیند نوتری است. برای اثبات این امر و به دست‌آوردن سایر خواص دامنه‌های دد‌کیند، باید مفهوم ایده‌آل کسری را معرفی‌کنیم.

تعریف ۲۰۶ . فرض‌کنیم R یک‌دامنه‌ٔصحیح با میدان‌خارج‌قسمتی K باشد. هر ***ایده‌آل کسری*** R یک R ــ زیرمدول ناصفر I از K است به‌طوری‌که، به‌ازای‌عنصر ناصفری چون $a \in R$، $aI \subset R$.

مثال. هر ایده‌آل ناصفر معمولی I در دامنهٔ صحیح R یک R ــ زیرمدول R ، و درنتیجه یک ایده‌آل کسری R ، می‌باشد. بـه عکس، هر ایده‌آل کسری R که مشمول R باشد یک ایده‌آل معمولی R است.

مثال. هر Rــ زیرمدول ناصفر بـا تولید متناهی I از K یک ایده‌آل کسری R است. زیرا هرگاه I به وسیلهٔ $b_1, \ldots, b_n \in K$ تولید شود، آنگاه $I = Rb_1 + \cdots + Rb_n$ و، به‌ازای هر i ، $b_i = c_i/a_i$ ، که در آن $c_i \in R$ ، $0 \neq a_i$. فرض کنیم $a = a_1a_2\cdots a_n$. در این صورت، $a \neq 0$ و $aI = Ra_2\cdots a_nc_1 + \cdots + Ra_1\cdots a_{n-1}c_n \subset R$.

تبصره. هرگاه I یک ایده‌آل کسری از دامنهٔ R بوده و $aI \subset R$ $(0 \neq a \in R)$ ، آنگاه aI یک ایده‌آل معمولی در R است و نگاشت $I \to aI$ داده شده با $x \mapsto ax$ یک یکریختی R ــ مدولهاست.

قضیهٔ ۳.۶. هرگاه R یک دامنهٔ صحیح با میدان خارج‌قسمتی K باشد، آنگاه مجموعهٔ تمام ایده‌آلهای کسری R یک تگگون تعویضپذیر تشکیل می‌دهد، که در آن R همانی بوده و ضرب با $IJ = \left\{\sum_{i=1}^{n} a_ib_i \mid a_i \in I;\ b_i \in J;\ n \in \mathbf{N}^*\right\}$ **داده شده است.**

برهان. تمرین؛ توجه کنیـد کـه هرگاه I و J ایده‌آلهایی در R باشند، آنگاه IJ حاصلضرب معمولی ایده‌آلها می‌باشد.

گوییم ایـده‌آل کسـری I از دامنهٔ صحیح R **معکوسپذیر** است اگر به‌ازای ایده‌آل کسری چون J از R ، $IJ = R$. لذا، ایده‌آلهای کسری معکوسپذیر[1] آنهایی هستند که در تگگون تمام ایده‌آلهای کسری معکوس دارند.

چند تبصره. (یک) معکوس ایـده‌آل کسری معکوسپذیر I منحصر به فرد بوده و مساوی

---

۱. در نوشتجات گاهـی *ایده‌آلهای کسری معکوسپذیر فقط ایده‌آلهای معکوسپذیر نامیده شده‌اند.*

است با $I^{-1} = \{a \in K \mid aI \subset R\}$. درواقع، به ازای هر ایده‌آل کسری I، مجموعهٔ $I^{-1} = \{a \in K \mid aI \subset R\}$ یک ایده‌آل کسری است به‌طوری که $I^{-1}I = II^{-1} \subset R$ هرگاه I معکوسپذیر بوده و $IJ = JI = R$ ، آنگاه بوضوح $J \subset I^{-1}$. به عکس، چون I^{-1} و J ، Rـ زیرمدولهایی از K اند ، $I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subset JR = RJ \subset J$ ، که از آنجا $J = I^{-1}$.

(دو) هرگاه I, A, B ایده‌آلهای کسری R باشند به‌طوری‌که $IA = IB$ و I معکوسپذیر باشد ، آنگاه $A = RA = (I^{-1}I)A = I^{-1}(IB) = RB = B$.

(سه) هرگاه I یک ایده‌آل معمولی در R باشد ، آنگاه $R \subset I^{-1}$.

مثال. هر ایده‌آل اصلی ناصفر در دامنهٔ صحیح R معکوسپذیر است . اگر K میدان خارج‌قسمتی R بوده و $I = (b)$ که در آن $b \neq 0$ ، فرض می‌کنیم $J = Rc \subset K$ ، که در آن $c = 1_K/b$. در این صورت ، J ایده‌آل کسری R است به‌طوری که $IJ = R$.

ایده‌آلهای کسری معکوسپذیر در توصیف دامنه‌های دد کیند نقشی کلیدی دارند. پنج نتیجهٔ زیر نکاتی در باب آنها می‌باشند .

لم ۴۰۶ . *فرض کنیم $I, I_1, I_2, \ldots, I_n$ ایده‌آلهایی در دامنهٔ صحیح R باشند .*

(یک) ایده‌آل $I_1 I_2 \cdots I_n$ معکوسپذیر است اگر و فقط اگر هر I_j معکوسپذیر باشد .

(دو) هرگاه $P_1 \cdots P_m = I = Q_1 \cdots Q_n$ ، که در آن P_i و Q_j ایده‌آلهای اولی در R بوده و هر P_i معکوسپذیر باشد ، آنگاه $m = n$ و (پس از اندیسگذاری مجدد) ، به‌ازای هر $i = 1, \ldots, m$ ، $P_i = Q_i$.

برهان. (یک) هرگاه J ایده‌آلی کسری باشد به‌طوری که $J(I_1 \cdots I_n) = R$ ، آنگاه ، به‌ازای هر $j = 1, 2, \ldots, n$ ، $I_j(JI_1 \cdots I_{j-1} I_{j+1} \cdots I_n) = R$ ، که از آنجا I_j معکوسپذیر است . به عکس، هرگاه هر I_j معکوسپذیر باشد ، آنگاه $(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = R$ ، که از آنجا $I_1 \cdots I_n$ معکوسپذیر است .

(دو) برهان به‌استقرا بر m است و حالت $m = 1$ به خواننده محول می‌شود . اگر $m > 1$ ، یکی از P_i ها ، مثلا " P_1 " ، را طوری می‌گیریم که P_1 حقیقتا "شامل P_i به‌ازای $i = 2, \ldots, m$ نباشد . چون $Q_1 \cdots Q_n = P_1 \cdots P_m \subset P_1$ و P_1 اول است ، Q_i ای ، مثلا " Q_1 " ، مشمول P_1 می‌باشد (تعریف III ۱۴۰۲۰) . به همین نحو ، چون $P_1 \cdots P_m = Q_1 \cdots Q_n \subset Q_1$ ،

به‌ازای i ی، $P_i \subset Q_1$. از اینرو، $P_i \subset Q_1 \subset P_1$. بنابر مینیمالی P_1 ، باید داشته باشیم $P_i = Q_1 = P_1$. چون $P_1 = Q_1$ معکوسپذیراست، تبصرهٔ (دو) بعد از قضیهٔ ۳۰۶ ایجاب می‌کند که

$$P_2P_3\cdots P_m = Q_2Q_3\cdots Q_n.$$

بنابراین، طبق فرض استقرا، $m = n$ و (پس‌ازاندیسگذاری‌مجدد)، به‌ازای $i = 1,2,\ldots,m$، $P_i = Q_i$.

مثال پیش از لم ۴۰۶ و قضیهٔ III ۴۰۳۰ نشان می‌دهد که هر ایده‌آل اول ناصفر در یک دامنهٔ ایده‌آل اصلی هم معکوسپذیر و هم ماکزیمال است. به‌طور کلی، داریم:

قضیهٔ ۵۰۶ . هرگاه R یک دامنهٔ دد کیند باشد، آنگاه هر ایده‌آل اول ناصفر R معکوسپذیر و ماکزیمال است.

برهان. ابتدانشان می‌دهیم هرایده‌آل‌اول معکوسپذیر P ماکزیمال است. اگر $a \in R - P$ ، باید نشان داد که ایده‌آل $P + Ra$ تولید شده به وسیلهٔ P و a مساوی R است. هرگاه $P + Ra \neq R$ ، آنگاه چون R دد کینداست، ایده‌آلهای‌اولی‌چون P_i و Q_i وجوددارند به‌طوری که $P + Ra = P_1P_2\cdots P_m$ و $P + Ra^2 = Q_1Q_2\cdots Q_n$. فرض‌کنیم $\pi : R \to R/P$ برووریختی کانونی بوده‌و ایده‌آلهای اصلی در R/P را درنظر می‌گیریم که به ترتیب با $\pi(a)$ و $\pi(a^2)$ تولید می‌شوند. واضح است که

$$(\pi(a)) = \pi(P_1)\cdots\pi(P_m) \quad \text{و} \quad (\pi(a^2)) = \pi(Q_1)\cdots\pi(Q_n) .$$

چون به‌ازای هر i ، $\ker\pi = P \subset P_i$ و $P \subset Q_i$ ، ایده‌آلهای $\pi(P_i)$ و $\pi(Q_i)$ در R/P اولند (تمرین III ۱۷۰۲۰ (آ)) . چون R/P یک دامنهٔ صحیح است (قضیهٔ III ۱۶۰۲۰)، هرایده‌آل‌اصلی در R/P معکوسپذیر است (ر.ک. مثال پیش از لم ۴۰۶) . درنتیجه، بنابر لم ۴۰۶ (یک)، $\pi(P_i)$ و $\pi(Q_i)$ معکوسپذیرند. چون

$$\pi(Q_1)\cdots\pi(Q_n) = (\pi(a^2)) = (\pi(a))^2 = \pi(P_1)^2\cdots\pi(P_m)^2,$$

لم ۴۰۶ (دو) ایجاب می‌کند که $n = 2m$ و (پس از اندیسگذاری مجدد)، به‌ازای $i = 1,2,\ldots,m$ ، $\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1})$. چون به‌ازای هر i ، $\operatorname{Ker}\pi = P \subset P_i$ و $P \subset Q_i$ ،

$$P_i = \pi^{-1}(\pi(P_i)) = \pi^{-1}(\pi(Q_{2i})) = Q_{2i}$$

و به همین نحو، به‌ازای $i = 1,2,\ldots,m$ ، $P_i = Q_{2i-1}$. درنتیجه، $P + Ra^2 = (P + Ra)^2$ و $P \subset P + Ra^2 \subset (P + Ra)^2 \subset P^2 + Ra$. هرگاه $(c \in P^2, r \in R)$ $b = c + ra \in P$ ، آنگاه $ra \in P$. لذا، $r \in P$ ، زیرا P اول‌است و $a \notin P$. بنابراین، $P \subset P^2 + Pa \subset P$ ، که ایجاب می‌کند که $P = P^2 + Pa = P(P + Ra)$. چون P معکوسپذیر است، $R = P^{-1}P = P^{-1}P(P + Ra) = R(P + Ra) = P + Ra$. این یک تناقض است. بنابراین، هر ایده‌آل اول معکوسپذیر P ماکزیمال می‌باشد.

حال فرض کنیم P ایده‌آل‌اول ناصفری در R بوده و c عنصر ناصفری از P باشد. پس به‌ازای ایده‌آلهای اولی چون P_i ، $(c) = P_1P_2\cdots P_n$. چون $P_1P_2\cdots P_n = (c) \subset P$ ، به‌ازای k ای داریم $P_k \subset P$ (تعریف III ۱۴.۲۰) . ایده‌آل‌اصلی (c) معکوسپذیر است؛ و درنتیجه، P_k نیز چنین است (لم ۴.۶ (یک)) . بنابر قسمت اول برهان، P_k ماکزیمال است، که از آنجا $P_k = P$. بنابراین، P ماکزیمال و معکوسپذیر است.

مثال. هرگاه F میدان‌باشد، آنگاه ایده‌آلهای اصلی (x_1) و (x_2) در دامنهٔ چندجمله‌ای $F[x_1,x_2]$ اولندولی ماکزیمال‌نیستند (زیرا $(x_i) \subsetneq (x_1,x_2) \subsetneq F[x_1,x_2]$) . درنتیجه، $F[x_1,x_2]$ دد کیند نیست (قضیهٔ ۵.۶) . چون $F[x_1,x_2]$ بنابر قضیهٔ ۹.۴ نوتری است، ردهٔ دامنه‌های دد کیند حقیقتا" مشمول ردهٔ دامنه‌های نوتری می‌باشد.

لم ۶.۶. *هرگاه I یک ایده‌آل‌کسری‌از دامنهٔ صحیح R با میدان خارج‌قسمتی K بوده و $f \in Hom_R(I,R)$ ، آنگاه، به‌ازای هر $a,b \in I$ ، $af(b) = bf(a)$.*

برهان. داریم $a = r/s$ و $b = v/t$ $(r,s,v,t \in R;\ s,t \neq 0)$ ؛ درنتیجه، $sa = r$ و $tb = v$. از اینرو، $sab = rb \in I$ و $tab = va \in I$. لذا، در R ، $sf(tab) = f(stab) = tf(sab)$. بنابراین، $af(b) = saf(b)/s = f(sab)/s = f(tab)/t = tbf(a)/t = bf(a)$.

لم ۷.۶. *هر ایده‌آل کسری‌معکوسپذیراز دامنهٔ صحیح R با میدان خارج‌قسمتی K یک R ــ مدول با تولید متناهی است.*

برهان. چون $I^{-1}I = R$ ، $a_i \in I^{-1}, b_i \in I$ ی وجوددارند به‌طوری که $1_R = \sum_{i=1}^{n} a_i b_i$. هرگاه $c \in I$ ، آنگاه $c = \sum_{i=1}^{n} (ca_i)b_i$. به‌علاوه، هر $ca_i \in R$ ، زیرا $a_i \in I^{-1} = \{a \in K \mid aI \subset R\}$.

بنابراین، I به عنوان یک R ــ مدول به وسیلهٔ $b_1, \ldots, b_n$ تولید می‌شود (قضیهٔ IV ۵۰۱۰ (سه)).

دیدیم که هر ایده‌آل ناصفر I در دامنهٔ ایده‌آل اصلی D معکوسپذیر است. به علاوه، به‌عنوان D ــ مدول، I با D یکریخت‌است (ر.ک. قضیهٔ IV ۵۰۱۰ (یک)). لذا، I یک D ــ مدول آزاد، و درنتیجه تصویری، می‌باشد. این نتیجه در دامنه‌های صحیح دلخواه نیز برقرار است.

قضیهٔ ۸۰۶. فرض کنیم R یک دامنهٔ صحیح بوده و I یک ایده‌آل کسری از R باشد. در این صورت، I معکوسپذیر است اگر و فقط اگر I یک R ــ مدول تصویری باشد.

برهان. ($\Leftarrow$) بنابرلم ۷۰۶ و قضیهٔ IV ۵۰۱۰ ، $I = Rb_1 + \cdots + Rb_n$ ، که در آن $b_i \in I$ و $1_R = \sum_{i=1}^{n} a_i b_i$ $(a_i \in I^{-1})$. فرض کنیم F یک R ــ مدول آزاد با پایه‌ای مرکب از n عنصر $e_1, \ldots, e_n$ باشد. در این‌صورت، نگاشت $\pi : F \to I$ تعریف شده با $e_i \mapsto b_i$ یک بروریختی R ــ مدولهاست (ر.ک. قضیهٔ IV ۱۰۲۰)، و یک دنبالهٔ کامل کوتاه مانند $0 \to \operatorname{Ker}\pi \to F \xrightarrow{\pi} I \to 0$ وجود دارد. $\zeta : I \to F$ را با $\zeta(c) = ca_1e_1 + \cdots + ca_ne_n$ $(c \in I)$ تعریف و تحقیق کنید ζ یک همریختی R ــ مدولهاست به‌طوری که $\pi\zeta = 1_I$ (توجه کنید که به‌ازای هر i ، $ca_i \in R$ ، زیرا $a_i \in I^{-1}$). درنتیجه، دنبالهٔ کامل تجزیه شده و I یک جمعوند مستقیم یک R ــ مدول آزاد است (قضیهٔ IV ۱۸۰۱۰). بنابراین، طبق قضیهٔ IV ۴۰۳۰ ، I تصویری است.

($\Rightarrow$) فرض کنیم $X = \{b_j \mid j \in J\}$ یک مجموعهٔ (احتمالاً نامتناهی) از مولدهای ناصفر از R ــ مدول تصویری I باشد. همچنین، b_0 عنصر ثابتی از X باشد. و نیز F یک R ــ مدول آزاد با پایهٔ $\{e_j \mid j \in J\}$ بوده و $\phi : F \to I$ یک بروریختی از R ــ مدولها تعریف

شده با $e_i \mapsto b_i$ باشد (قضیهٔ IV ۱۰۲۰) . چون I تصویری است ، یک همریختی R ــ مدولها مانند $\psi : I \to F$ وجود دارد به‌طوری که $\phi\psi = 1_I$. به‌ازای هر $j \in J$ ، فرض کنیم $\pi_j : F \to Re_j \cong R$ تصویر کانونیی باشد که $\sum_i r_i e_i \in F$ را به روی $r_j \in R$ بنگارد (ر.ک. قضیهٔ IV ۱۰۲۰) . در این صورت ، به‌ازای هر j ، نگاشت $\theta_j = \pi_j\psi : I \to R$ یک همریختی R ــ مدولهاست . فرض‌کنیم $c_j = \theta_j(b_0)$. بنابرلم ۶.۶ ، به‌ازای هر $c \in I$ ، $cc_j = c\theta_j(b_0) = b_0\theta_j(c)$ ؛ درنتیجه ، در میدان خارج‌قسمتی K از R ،

$$c(c_j/b_0) = cc_j/b_0 = b_0\theta_j(c)/b_0 = \theta_j(c) \in R.$$

بنابراین ،

$$c_j/b_0 \in I^{-1} = \{a \in K \mid aI \subset R\}.$$

درنتیجه ، به‌ازای هر $c \in I$ ،

$$\psi(c) = \sum_{j \in J_1} \theta_j(c)e_j = \sum_{j \in J_1} c(c_j/b_0)e_j,$$

که در آن J_1 زیرمجموعهٔ متناهی $\{j \in J \mid \theta_j(c) \neq 0\}$ است . بنابراین ، به‌ازای هر $c \in I$ ناصفر ،

$$c = \phi\psi(c) = \phi(\sum_{j \in J_1} c(c_j/b_0)e_j) = \sum_{j \in J_1} c(c_j/b_0)b_j = c(\sum_{j \in J_1} (c_j/b_0)b_j),$$

که از آنجا $1_R = \sum_{j \in J_1} (c_j/b_0)b_j$ که در آن $c_j/b_0 \in I^{-1}$. پس نتیجه می‌شود که $R \subset I^{-1}I$. چون $I^{-1}I \subset R$ همواره درست است ، $R = I^{-1}I$. بنابراین ، I معکوسپذیر می‌باشد .

توصیف دامنه‌های ددکیند داده‌شده در زیر نیاز به مفهوم دیگری دارد . هر *حلقهٔ ارزیابی گسسته* یک دامنهٔ ایده‌آل اصلی است که درست یک ایده‌آل اول ناصفر دارد (ایده‌آل صفر در هر دامنهٔ صحیح اول است) .

لم ۹.۶ . *هرگاه* R *یک دامنهٔ صحیح به‌طور بسته صحیح و نوتری بوده و* R *دارای ایده‌آل اول ناصفر منحصر به فرد* P *باشد ، آنگاه* R *یک حلقهٔ ارزیابی گسسته می‌باشد .*

برهان . کافی است نشان دهیم که هر ایده‌آل حقیقی در R اصلی است . این کار به مطالب زیر نیاز دارد ، که ذیلا" ثابت می‌شوند :

(یک) فرض کنیم K میدان خارج‌قسمتی R باشد. به‌ازای هر ایده‌آل کسری I از R، مجموعهٔ $\{a \in K \mid aI \subset I\}$ درست مساوی R است؛

(دو) $R \subsetneq P^{-1}$؛

(سه) P معکوسپذیر است؛

(چهار) $\bigcap_{n \in N^*} P^n = 0$؛

(پنج) P اصلی است.

حال قسمتهای (یک) تا (چهار) را فرض کرده، I را ایده‌آلی حقیقی از R می‌گیریم. در این‌صورت، I مشمول یک ایده‌آل ماکزیمال ناصفر M از R است (قضیهٔ III ۱۸.۲۰)، که لزوماً "اول" می‌باشد (قضیهٔ III ۱۹.۲۰). بنابر یکتایی، $M = P$؛ درنتیجه، $I \subset P$. چون طبق (چهار) $\bigcap_{n \in N^*} P^n = 0$، بزرگترین عدد صحیح m وجود دارد به‌طوری که $I \subset P^m$ و $I \not\subset P^{m+1}$. $b \in I - P^{m+1}$ را اختیار می‌کنیم. چون طبق (پنج) به‌ازای $a \in R$ ای، $P = (a)$، پس $P^m = (a)^m = (a^m)$. و چون $b \in P^m$، پس $b = ua^m$. به علاوه، $u \notin P = (a)$ (در غیر این صورت، $b \in P^{m+1} = (a^{m+1})$). درنتیجه، u یک یکه در R است (در غیر این صورت، طبق قضیهٔ III ۲۰.۳۰، (u) یک ایده‌آل حقیقی است؛ و لذا، طبق استدلال فوق، مشمول P می‌باشد). بنابراین، طبق قضیهٔ III ۲۰.۳۰، $P^m = (a^m) = (ua^m) = (b) \subset I$، که از آنجا I ایده‌آل اصلی $P^m = (a^m)$ می‌باشد.

احکام (یک) تا (پنج) به صورت زیر تحقیق می‌شوند.

(یک) واضح است که $R \subset I$. به آسانی معلوم می‌شود که I زیرحلقه‌ای از K و یک ایده‌آل کسری R است، که از آنجا I (به عنوان R ــ مدول) با ایده‌آلی از R یکریخت است (تبصرهٔ پیش از قضیهٔ ۳.۶). لذا، چون R نوتری است، I با تولید متناهی می‌باشد (قضیهٔ ۹.۱). قضیهٔ ۳.۵ (به‌ازای $T = I$) ایجاب می‌کند که هر عنصر I روی R صحیح باشد. بنابراین، $I \subset R$ زیرا R به‌طور صحیح بسته است. از اینرو، $I = R$.

(دو) به یاد آورید که به‌ازای هر ایده‌آل J در R، $R \subset J^{-1}$. فرض کنیم $\mathfrak{F}$ مجموعهٔ تمام ایده‌آلهای J در R باشد به‌طوری که $R \subsetneq J^{-1}$. چون P یک ایده‌آل حقیقی است (تعریف III ۱۴.۲۰)، بنابر قضیهٔ III ۲۰.۳۰، هر عنصر ناصفر P یک غیر یکه است.

هرگاه $J=(a)$ $(0\neq a\in P)$ ، آنگاه $1_R/a\in J^{-1}$ ولی $1_R/a\notin R$ ، که از آنجا $R\subsetneq J^{-1}$. بنابراین، $\mathfrak{F}$ ناتهی است. چون R نوتری است، $\mathfrak{F}$ شامل عنصر ماکزیمال M می‌باشد (قضیهٔ ۴۰۱) . حکم می‌کنیم که M یک ایده‌آل اول R است. اگر $ab\in M$ که $a,b\in R$ و $a\notin M$ ، $c\in M^{-1}-R$ را اختیار می‌کنیم. در این صورت، $c(ab)\in R$ ، که از آنجا $bc(aR+M)\subset R$ و $bc\in(aR+M)^{-1}$. بنابراین، $bc\in R$ (در غیر این صورت، $aR+M\in\mathfrak{F}$ ، که با ماکزیمالی M متناقض است) . درنتیجه $c(bR+M)\subset R$ ؛ و لذا، $c\in(bR+M)^{-1}$. چون $c\notin R$ ، ماکزیمالی M ایجاب می‌کند که $bR+M=M$ ، که از آنجا $b\in M$. بنابراین، طبق قضیهٔ III ۱۵۰۲۰ ، M اول است. چون $M\neq 0$ ، بنابر یکتایی باید داشته باشیم $P=M$. لذا، $R\subsetneq M^{-1}=P^{-1}$.

(سه) واضح است که $P\subset PP^{-1}\subset R$. استدلال بند اول برهان نشان می‌دهد که P ایده‌آل ماکزیمال منحصر به فردی در R است، که از آنجا $P=PP^{-1}$ یا $PP^{-1}=R$. اما هرگاه $P=PP^{-1}$ ، آنگاه $P^{-1}\subset\bar{P}$ و، بنابر (یک) و (دو)، $\bar{P}=R$ ، که یک تناقض می‌باشد. بنابراین، $PP^{-1}=R$ و P معکوسپذیر است.

(چهار) هرگاه $\bigcap_{n\in N^*}P^n\neq 0$ ، آنگاه $\bigcap_{n\in N^*}P^n$ یک ایده‌آل کسری R است. تحقیق کنید که $P^{-1}\subset\overline{\bigcap_{n\in N^*}P^n}$. در این صورت، طبق (یک) و (دو)، $R\subsetneq P^{-1}\subset\overline{\bigcap_{n\in N^*}P^n}=R$ ، که یک تناقض است.

(پنج) $a\in P$ ای وجود دارد به‌طوری که $a\notin P^2$ (در غیر این صورت، $P=P^2$ ، که از آنجا $\bigcap_{n\in N^*}P^n=P\neq 0$ که با (چهار) متناقض است) . پس aP^{-1} ایده‌آل ناصفری در R است به‌طوری که $aP^{-1}\not\subset P$ (در غیر این صورت، $a\in aR=aP^{-1}P\subset P^2$) . بند اول برهان نشان می‌دهد که هر ایده‌آل حقیقی در R مشمول P است، که از آنجا $aP^{-1}=R$. بنابراین، طبق قسمت (سه)، $(a)=(a)R=(a)P^{-1}P=(aP^{-1})P=RP=P$.

قضیهٔ ۱۰۰۶ . *شرایط زیر بر دامنهٔ صحیح R با هم معادلند:*

(یک) R یک دامنهٔ دد کیند است؛

(دو) هر ایده‌آل حقیقی در R حاصلضرب منحصر به فردی است از چند ایده‌آل اول؛

(سه) هر ایده‌آل ناصفر در R معکوسپذیر است؛

(چهار) هر ایده‌آل کسری R معکوسپذیر است؛

(پنج) مجموعهٔ تمام ایده‌آلهای کسری R تحت ضرب یک گروه است ؛
(شش) هر ایده‌آل در R تصویری است ؛
(هفت) هر ایده‌آل کسری R تصویری است ؛
(هشت) R نوتری و به‌طور صحیح بسته است و هر ایده‌آل اول ناصفر ماکزیمال است ؛
(نه) R نوتری است و به‌ازای هر ایده‌آل اول ناصفر P از R ، موضعی سازی R_P از R در P یک حلقهٔ ارزیابی گسسته است .

برهان . معادل بودن (پنج) ⇔ (چهار) بدیهی است (ر.ک. قضیهٔ ۳.۶) .
(دو) ⇒ (یک) و (سه) ⇒ (دو) از لم ۴.۶ و قضیهٔ ۵.۶ نتیجه می‌شوند .
(شش) ⇔ (سه) و (چهار) ⇔ (هفت) نتایج فوری قضیهٔ ۸.۶ می‌باشند.
(هفت) ⇒ (شش) از تبصرهٔ پیش‌از قضیهٔ ۳.۶ نتیجه می‌شود . برای اتمام برهان فقط باید استلزامهای (هشت) ⇒ (چهار)، (نه) ⇒ (هشت) ، و (یک) ⇒ (نه) را ثابت کنیم .

(هشت) ⇒ (چهار) بنابر (چهار) ، هر ایده‌آل R معکوسپذیر است ؛ و درنتیجه ، بنابر لم ۷.۶ ، با تولید متناهی است . بنابراین ، طبق قضیهٔ ۹.۱ ، R نوتری است . فرض کنیم K میدان خارج‌قسمتی R باشد . هرگاه $u \in K$ روی R صحیح باشد ، آنگاه ، طبق قضیهٔ ۳.۵ ، $R[u]$ یک R ـ زیرمدول با تولید متناهی از K است . درنتیجه ، مثال دوم بعداز تعریف ۲.۶ نشان می‌دهد که $R[u]$ یک ایده‌آل کسری R است . بنابراین ، طبق قسمت (چهار) ، $R[u]$ معکوسپذیر است . لذا ، چون $R[u]R[u] = R[u]$ ، داریم

$$R[u] = RR[u] = (R[u]^{-1}R[u])R[u] = R[u]^{-1}R[u] = R$$

که از آنجا $u \in R$. بنابراین ، R به‌طور صحیح بسته است . بالاخره ، هرگاه P یک ایده‌آل اول ناصفر در R باشد ، آنگاه یک ایده‌آل ماکزیمال M از R وجود دارد که شامل P است (قضیهٔ III ۱۸.۲۰) . بنابر (چهار) ، M معکوسپذیر است . درنتیجه ، $M^{-1}P$ یک ایده‌آل کسری از R با خاصیت $M^{-1}P \subset M^{-1}M = R$ می‌باشد ؛ لذا ، $M^{-1}P$ ایده‌آلی در R می‌باشد . چون $M(M^{-1}P) = RP = P$ و P اول است ، یا $M \subset P$ یا $M^{-1}P \subset P$. اما هرگاه $M^{-1}P \subset P$ ، آنگاه $R \subset M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subset PP^{-1} \subset R$ ، که از آنجا $M^{-1} = R$. لذا ،

$$R = MM^{-1} = MR = M$$

که با ماکزیمال بودن M متناقض است. بنابراین، $M \subset P$؛ و در نتیجه، $M = P$. بنابراین، P ماکزیمال می‌باشد.

(نه) $\Rightarrow$ (هشت) بنابر قضیهٔ ۸۰۵، R_P یک دامنهٔ صحیح به‌طور صحیح بسته است. بنابر لم III ۹۰۴۰، هر ایده‌آل در R_P به شکل $I_P = \{i/s \mid i \in I; s \notin P\}$ است، که در آن I ایده‌آلی از R است. چون هر ایده‌آل R طبق (هشت) و قضیهٔ ۹۰۱ با تولید متناهی است، نتیجه می‌شود که هر ایده‌آل R_P با تولید متناهی است. بنابراین، طبق قضیهٔ ۹۰۱، R_P نوتری است. بنابر قضیهٔ III ۱۱۰۴۰، هر ایده‌آل اول ناصفر R_P به شکل I_P است، که در آن I یک ایده‌آل اول ناصفر R است که مشمول P می‌باشد. چون هر ایده‌آل اول ناصفر R طبق (هشت) ماکزیمال است، P_P باید ایده‌آل اول ناصفر منحصر به فردی در R_P باشد. بنابراین، طبق لم ۹۰۶، R_P یک حلقهٔ ارزیابی گسسته می‌باشد.

(یک) $\Rightarrow$ (نه) ابتدا نشان می‌دهیم که هر ایده‌آل I $(\neq 0)$ معکوسپذیر است. II^{-1} یک ایده‌آل کسری از R مشمول در R است (تبصرهٔ (یک) بعد از قضیهٔ ۳۰۶)؛ در نتیجه، II^{-1} ایده‌آلی در R می‌باشد. هرگاه $II^{-1} \neq R$، آنگاه ایده‌آل ماکزیمالی چون M شامل II^{-1} وجود دارد (قضیهٔ III ۱۸۰۲۰). چون M اول است (قضیهٔ III ۱۹۰۲۰)، بنابر (نه)، ایده‌آل I_M در R_M اصلی است؛ مثلاً "$I_M = (a/s)$"، که در آن $a \in I$ و $s \in R - M$. چون R نوتری است، طبق قضیهٔ ۹۰۱، I با تولید متناهی است؛ مثلاً "$I = (b_1, \ldots, b_n)$". به‌ازای هر i، $b_i/1_R \in I_M$؛ لذا، در R_M، به‌ازای $s_i \in R - M$ ی $r_i \in R$ و $(r_i/s_i)(a/s)$، $b_i/1_R =$. بنابراین، $s_i s b_i = r_i a \in I$. فرض کنیم $t = ss_1s_2\cdots s_n$. چون $R - M$ ضربی است، $t \in R - M$. در میدان خارج‌قسمتی R، به‌ازای هر i داریم $(t/a)b_i = tb_i/a = s_1\cdots s_{i-1}s_{i+1}\cdots s_n r_i a \in I \subset R$، که از آنجا $t/a \in I^{-1}$. در نتیجه، $I = (t/a)a \in I^{-1}I \subset M$، که با $t \in R - M$ متناقض می‌باشد. بنابراین، $II^{-1} = R$ و I معکوسپذیر می‌باشد.

به‌ازای هر ایده‌آل I $(\neq R)$ از R، ایده‌آل ماکزیمال M_I از R را طوری می‌گیریم که $I \subset M_I \subsetneq R$ (قضیهٔ III ۱۸۰۲۰؛ اصل انتخاب). اگر $I = R$، فرض می‌کنیم $M_R = R$. در این صورت، IM_I^{-1} یک ایده‌آل کسری R با خاصیت

$$IM_I^{-1} \subset M_I M_I^{-1} \subset R$$

است. بنابراین، IM_I^{-1} ایده‌آلی از R است که بوضوح شامل I می‌باشد. همچنین،

هرگاه I حقیقی باشد، آنگاه $I \subsetneq IM_I^{-1}$ (درغیراین‌صورت، چون I و M_I معکوسپذیرند، $R = RR = (I^{-1}I)(M_I^{-1}M_I) = I^{-1}(IM_I^{-1})M_I = I^{-1}IM_I = RM_I = M_I$، که با انتخاب M_I متناقض می‌باشد). فرض کنیم S مجموعهٔ تمام ایده‌آلهای R باشد و تابع $f: S \to S$ را با $I \mapsto IM_I^{-1}$ تعریف می‌کنیم. اگر J یک ایده‌آل حقیقی باشد، بنابر قضیهٔ بازگشتی ۲.۶ در آشنایی (با f به‌ازای هر n) تابعی مانند $\phi: \mathbf{N} \to S$ وجود دارد به‌طوری که $\phi(0) = J$ و $\phi(n+1) = f(\phi(n))$. هرگاه $\phi(n)$ را با J_n و M_{J_n} را با M_n نشان دهیم، آنگاه زنجیر افزایشی $J = J_0 \subset J_1 \subset J_2 \subset \cdots$ از ایده‌آلها را داریم به‌طوری که $J = J_0$ و $J_{n+1} = f(J_n) = J_nM_n^{-1}$. چون R نوتری و J حقیقی است، کوچکترین عدد صحیحی مانند k هست به‌طوری که

$$J = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_{k-1} \subsetneq J_k = J_{k+1}.$$

لذا، $J_k = J_{k+1} = f(J_k) = J_kM_k^{-1}$ تبصره‌های بالا نشان می‌دهند که این می‌تواند فقط وقتی رخ دهد که $J_k = R$. درنتیجه $R = J_k = f(J_{k-1}) = J_{k-1}M_{k-1}^{-1}$، که از آنجا

$$J_{k-1} = J_{k-1}R = J_{k-1}M_{k-1}^{-1}M_{k-1} = RM_{k-1} = M_{k-1}.$$

چون $M_{k-1} = J_{k-1} \subsetneq J_k = R$، پس M_{k-1} ایده‌آل ماکزیمال است. مینیمالی k تضمین می‌کند که هر کدام از $M_0, \ldots, M_{k-2}$ نیز ماکزیمال‌است (در غیر این صورت، $M_i = R$، که از آنجا $J_{j+1} = J_jM_j^{-1} = J_jR^{-1} = J_jR = J_j$). به‌آسانی تحقیق می‌شود که

$$M_{k-1} = J_{k-1} = J_{k-2}M_{k-2}^{-1} = J_{k-3}M_{k-3}^{-1}M_{k-2}^{-1} = \cdots = JM_0^{-1}M_1^{-1}\cdots M_{k-2}^{-1}.$$

درنتیجه، چون هر M_i معکوسپذیر است،

$$M_{k-1}(M_0\cdots M_{k-2}) = JM_0^{-1}\cdots M_{k-2}^{-1}(M_0\cdots M_{k-2}) = J.$$

لذا، J حاصلضرب ایده‌آلهای ماکزیمال (درنتیجه، اول) است. بنابراین، R ددکیند می‌باشد.

بحث را با مثالی خاتمه می‌دهیم که نشان می‌دهد که ردهٔ دامنه‌های ایده‌آل اصلی حقیقتاً مشمول ردهٔ دامنه‌های ددکیند است.

مثال. دامنهٔ صحیح $\mathbf{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a,b \in \mathbf{Z}\}$ دارای میدان خارج‌قسمتی $\mathbf{Q}(\sqrt{10}) = \{r + s\sqrt{10} \mid r,s \in \mathbf{Q}\}$ است. محاسبات خسته‌کننده و نظریهٔ مقدماتی اعداد نشان می‌دهند که $\mathbf{Z}[\sqrt{10}]$ به‌طور صحیح بسته است (تمرین ۱۴). چون نگاشت ارزیابی

$\mathbf{Z}[x] \to \mathbf{Z}[\sqrt{10}]$ داده شده با $f(x) \mapsto f(\sqrt{10})$ یک برووریختی و $\mathbf{Z}[x]$ نوتری است (قضیهٔ ۹۰۴)، $\mathbf{Z}[\sqrt{10}]$ نیز نوتری می‌باشد (تمرین ۵۰۱). بالاخره، اثبات اینکه هر ایده‌آل اول ناصفر $\mathbf{Z}[\sqrt{10}]$ ماکزیمال است مشکل نیست (تمرین ۱۵). بنابراین، طبق قضیهٔ ۱۰۶ (هشت)، $\mathbf{Z}[\sqrt{10}]$ یک دامنهٔ دد کیند می‌باشد. اما $\mathbf{Z}[\sqrt{10}]$ یک دامنهٔ ایده‌آل اصلی نیست (قضیهٔ III ۷۰۳۰ و تمرین III ۴۰۳۰).

تمرینات

۱. ایده‌آل تولید شده به وسیلهٔ 3 و $1 + \sqrt{5}i$ در زیر دامنهٔ $\mathbf{Z}[\sqrt{5}i]$ از $\mathbf{C}$ معکوسپذیر است.

۲. هر ایده‌آل معکوسپذیر در یک دامنهٔ صحیح که حلقهٔ موضعی باشد اصلی است.

۳. هرگاه I یک ایده‌آل معکوسپذیر در دامنهٔ صحیح R بوده و S مجموعه‌ای ضربی در R باشد که $0 \notin S$، آنگاه $S^{-1}I$ در $S^{-1}R$ معکوسپذیر است.

۴. فرض کنید R حلقه‌ای یکدار بوده و P یک Rـ مدول باشد. در این صورت، P تصویری است اگر و فقط اگر مجموعه‌هایی چون $\{a_i \mid i \in I\} \subset P$ و $\{f_i \mid i \in I\} \subset \mathrm{Hom}_R(P,R)$ موجود باشند به طوری که به ازای هر $a \in P$، $a = \sum_{i \in I} f_i(a)a_i$. [ر.ک. برهان قضیهٔ ۱۰۸۰۶]

۵. (عکس لم ۹۰۶) حلقهٔ ارزیابی گسستهٔ R نوتری و به‌طور صحیح بسته است.
[**راهنمایی.** تمرین ۵۰۸۰]

۶. (آ) هرگاه هر ایده‌آل اول در دامنهٔ صحیح R معکوسپذیر باشد، آنگاه R دد کیند است.

(ب) هرگاه R یک دامنهٔ صحیح نوتری باشد که در آن هر ایده‌آل ماکزیمال معکوسپذیر است، آنگاه R دد کیند می‌باشد.

۷. هرگاه S زیرمجموعه‌ای ضربی از دامنهٔ دد کیند R باشد (با $1_R \in S, 0 \notin S$)، آنگاه $S^{-1}R$ یک دامنهٔ دد کیند است.

۸. هرگاه R یک دامنهٔ صحیح بوده و P ایده‌آل اولی در $R[x]$ باشد به‌طوری که $P \cap R = 0$، آنگاه $R[x]_P$ یک حلقهٔ ارزیابی گسسته است.

۹. اگر دامنهٔ دد کیند R فقط تعدادی متناهی ایده‌آل اول ناصفر مانند $P_1, \ldots, P_n$

داشته باشد، آنگاه R یک دامنهٔ ایده‌آل اصلی می‌باشد.

[**راهنمایی.** $a_i \in P_i - P_i^2$ ی وجود دارد و، بنابر قضیهٔ باقیماندهٔ چینی III ۲۵۰۲۰، $b_i \in P_i$ ی موجوداست به‌طوری‌که، به‌ازای $j \neq i$، $b_i \equiv a_i \pmod{P_i}$ و $b_i \equiv 1_R \pmod{P_j}$. نشان دهید $P_i = (b_i)$، که ایجاب می‌کند که هر ایده‌آل اصلی باشد.]

۱۰. هرگاه I ایده‌آلی ناصفر در دامنهٔ ددکیند R باشد، آنگاه R/I یک حلقهٔ آرتینی می‌باشد.

۱۱. هر ایده‌آل حقیقی در دامنهٔ ددکیند را می‌توان با حداکثر دو عنصر تولید کرد.

۱۲. R ــ مدول A بخشپذیر است اگر به‌ازای جمیع $r \in R$ های ناصفر، $rA = A$. اگر R یک دامنهٔ ددکیند باشد، هر R ــ مدول بخشپذیر انژکتیو است. [عکس مطلب نیز درست است ولی مشکلتر می‌باشد.]

۱۳. (نابدیهی) هرگاه R یک دامنهٔ ددکیند با میدان خارج‌قسمتی K، F یک توسیع میدان بابعد متناهی از K، و S بست صحیح R در F (یعنی، حلقهٔ تمام عناصر F که روی R صحیح‌اند) باشد، آنگاه S یک دامنهٔ ددکیند می‌باشد.

۱۴. (آ) ثابت کنید که دامنهٔ صحیح $\mathbf{Z}[\sqrt{10}]$ یک توسیع صحیح از حلقهٔ $\mathbf{Z}$ بامیدان خارج‌قسمتی $\mathbf{Q}(\sqrt{10})$ است.

(ب) فرض کنید $u \in \mathbf{Q}(\sqrt{10})$ روی $\mathbf{Z}[\sqrt{10}]$ صحیح باشد. در این صورت، u روی $\mathbf{Z}$ صحیح است (قضیهٔ ۶۰۵). به علاوه، هرگاه $u \in \mathbf{Q}$، آنگاه $u \in \mathbf{Z}$ (تمرین ۸۰۵). ثابت کنید هرگاه $u \in \mathbf{Q}(\sqrt{10})$ و $u \notin \mathbf{Q}$، آنگاه u ریشهٔ یک چندجمله‌ای تکین تحویل‌ناپذیر از درجهٔ 2 در $\mathbf{Z}[x]$ است.

[**راهنمایی.** نتیجهٔ III ۱۳۰۶۰ و قضیهٔ ۶۰۱۰ V.]

(پ) ثابت کنید هرگاه $u = r + s\sqrt{10} \in \mathbf{Q}(\sqrt{10})$ و u ریشه‌ای از $x^2 + ax + b \in \mathbf{Z}[x]$ باشد، آنگاه $a = -2r$ و $b = r^2 - 10s^2$. [**راهنمایی.** توجه کنید که $u^2 - 2ru + (r^2 - 10s^2) = 0$؛ اگر $u \notin \mathbf{Q}$، از قضیهٔ ۶۰۱۰ V استفاده نمایید.]

(ت) ثابت کنید $\mathbf{Z}[\sqrt{10}]$ به‌طور صحیح بسته است. [**راهنمایی.** هرگاه $u = r + s\sqrt{10} \in \mathbf{Q}(\sqrt{10})$ ریشه‌ای از $x^2 + ax + b \in \mathbf{Z}[x]$ بوده‌و u زوج باشد، آنگاه طبق (پ)، $r \in \mathbf{Z}$؛ پس نتیجه می‌شود که $s \in \mathbf{Z}$. فرض فرد بودن a به تناقض می‌انجامد.]

۱۵ . (آ) هرگاه P ایده‌آل اول ناصفری از حلقهٔ $\mathbf{Z}[\sqrt{10}]$ باشد، آنگاه $P \cap \mathbf{Z}$ یک ایده‌آل اول ناصفر $\mathbf{Z}$ است. [**راهنمایی .** هرگاه $0 \neq u \in P$ ، آنگاه، طبق تمرین ۱۴ ، $x^2 + ax + b \in \mathbf{Z}[x]$. نشان دهیدکه یکی از a,b ها ناصفر بوده و در P قرار دارد .]

(ب) هر ایده‌آل اول ناصفر $\mathbf{Z}[\sqrt{10}]$ ماکزیمال است . [از قسمت (آ) قضیهٔ III ۴.۳۰ و استدلال مستقیم آسان یا قضیهٔ ۱۲.۵ استفاده نمایید .]

۱۶ . هر ***دامنهٔ ارزیابی*** یک دامنهٔ صحیح مانند R است به‌طوری که به‌ازای هر $a,b \in R$ ، $a \mid b$ یا $b \mid a$. (واضح است که هرحلقهٔ ارزیابی گسسته یک‌دامنهٔ ارزیابی است .) هر ***دامنهٔ پروفر***[1] یک دامنهٔ صحیح است که در آن هر ایده‌آل با تولید متناهی معکوسپذیر است .

(آ) احکام زیرباهم معادلند : (یک) R یک دامنهٔ پروفر است ؛ (دو) به‌ازای هر ایده‌آل اول P در R ، R_P یک دامنهٔ ارزیابی است ؛ (سه) به‌ازای هر ایده‌آل ماکزیمال M در R ، R_M یک دامنهٔ ارزیابی است .

(ب) یک دامنهٔ پروفر ددکیند است اگر و فقط اگر نوتری باشد .

(پ) هرگاه R یک دامنهٔ پروفر با میدان خارج‌قسمتی K باشد، آنگاه هر دامنهٔ S که $R \subset S \subset K$ پروفر است .

۷ قضیهٔ صفرهای هیلبرت

نتایج بخش VI ۱۰ و بخش ۵ را به کار برده نتیجهٔ مشهوری از هندسهٔ جبری کلاسیک ، یعنی قضیهٔ صفرهای هیلبرت ، را ثابت می‌کنیم . در طول راه لم نرمال‌سازی نوتر را نیز اثبات می‌نماییم . بابحث بسیار کوتاهی که زمینهٔ هندسی دارد آغاز می‌کنیم (این بحث در آخر بخش ادامه خواهد یافت) .

هندسهٔ جبری کلاسیک بررسی جوابهای همزمان دستگاههای معادلات چندجمله‌ای مانند

$$f(x_1, x_2, \ldots, x_n) = 0 \qquad (f \in S)$$

است ، که در آن K میدان بوده و $S \subset K[x_1, \ldots, x_n]$. جواب این دستگاه یک n تایی مانند $(a_1, \ldots, a_n) \in F^n = F \times F \times \cdots \times F$ (n عامل) است ، که در آن F یک توسیع

1. **Prüfer**

میدان به‌طور جبری بسته‌ٔ K بوده و، به‌ازای هر $f \in S$ ، $f(a_1, \ldots, a_n) = 0$. هر چنین جواب یک **صفر** S **در** F^n نام دارد. مجموعه‌ٔ تمام صفرهای S ، **K ــ واریته‌ٔ مستوی (یا مجموعه‌ٔ جبری)** در F^n نام دارد که با S تعریف و توسط $V(S)$ نموده می‌شود. لذا،

$$V(S) = \{(a_1, \ldots, a_n) \in F^n \mid f(a_1, \ldots, a_n) = 0 \text{ ، به‌ازای هر } f \in S\}$$

توجه کنید که هرگاه I ایده‌آل $K[x_1, \ldots, x_n]$ تولید شده به وسیلهٔ S باشد، آنگاه $V(I) = V(S)$.

انتساب $S \mapsto V(S)$ تابعی‌ازمجموعه‌ٔتمام‌زیرمجموعه‌های $K[x_1, \ldots, x_n]$ به مجموعه‌ٔ تمام زیرمجموعه‌های F^n تعریف می‌کند. به عکس، تابعی از مجموعه‌ٔ زیرمجموعه‌های F^n به مجموعه‌ٔ زیر مجموعه‌های $K[x_1, \ldots, x_n]$ به وسیله‌ٔ $Y \mapsto J(Y)$ تعریف می‌شود، که $Y \subset F^n$ و

$$J(Y) = \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ ، به‌ازای هر } (a_1, \ldots, a_n) \in Y\}$$

توجه کنید که $J(Y)$ عملاً یک ایده‌آل $K[x_1, \ldots, x_n]$ است. تناظر داده شده با V و J همان خواص صوری تناظر گالوا (اعمال پریمدار) بین میدانهای میانی یک توسیع و زیرگروههای گروه گالوا را دارد. به عبارت دیگر، مشابه زیر از لم ۶.۲۰ V را خواهیم داشت.

لم ۱۰۷ . فرض کنیم F یک توسیع میدان به‌طور جبری بسته از K بوده و S, T زیرمجموعه‌های $K[x_1, \ldots, x_n]$ و X, Y زیرمجموعه‌های F^n باشند. در این صورت،

(یک) $V(K[x_1, \ldots, x_n]) = \varnothing$; $J(F^n) = \varnothing$; $J(\varnothing) = K[x_1, \ldots, x_n]$ ؛

(دو) $S \subset T \Rightarrow V(T) \subset V(S)$ و $X \subset Y \Rightarrow J(Y) \subset J(X)$ ؛

(سه) $S \subset J(V(S))$ و $Y \subset V(J(Y))$ ؛

(چهار) $V(S) = V(J(V(S)))$ و $J(Y) = J(V(J(Y)))$.

برهان . تمرین.

طبیعی است سؤال شود که چه اشیایی تحت این تناظر **بسته‌اند**؛ یعنی، چه S و Y ی در $J(V(S)) = S$ و $V(J(Y)) = Y$ صدق می‌کنند. زیرمجموعه‌های‌بستهٔ $K[x_1, \ldots, x_n]$ به آسانی توصیف می‌شوند (تمرین ۲)، ولی توصیف زیرمجموعه‌های بستهٔ F^n نیاز به

قضیهٔ صفرها دارد، که می‌گوید به‌ازای هر ایده‌آل حقیقی I از $K[x_1, \ldots, x_n]$، $J(V(I)) = \mathrm{Rad}\, I$. برای اثبات قضیهٔ صفرها، به دو نتیجهٔ مقدماتی نیاز داریم، که اولین آنها بخودی خود جالب است.

قضیهٔ ۲۰۷ (لم نرمال‌سازی نوتر). *فرض کنیم R یک دامنهٔ صحیح باشد که توسیع حلقهٔ با تولید متناهی از میدان K است و r درجهٔ تعالی روی K ی میدان خارج‌قسمتی F از R باشد. در این صورت، یک زیرمجموعهٔ مستقل جبری مانند $\{t_1, t_2, \ldots, t_r\}$ از R وجود دارد به‌طوری که R روی $K[t_1, \ldots, t_r]$ صحیح است.*

برهان. فرض کنیم $R = K[u_1, \ldots, u_n]$؛ پس $F = K(u_1, \ldots, u_n)$. اگر $\{u_1, \ldots, u_n\}$ روی K مستقل جبری باشد، بنابر نتیجهٔ VI ۶.۱۰، $\{u_1, \ldots, u_n\}$ یک پایهٔ تعالی F روی K است، که‌ازآنجا $r = n$ و قضیه بداهتاً درست است. هرگاه $\{u_1, \ldots, u_n\}$ روی K وابستهٔ جبری باشد، آنگاه $r \leq n - 1$ (نتیجهٔ VI ۷.۱۰) و

$$\sum_{(i_1, \ldots, i_n) \in I} k_{i_1 \ldots i_n} u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n} = 0,$$

که در آن I یک مجموعهٔ متناهی از nتاییهای متمایز از اعداد صحیح نامنفی بوده و، به‌ازای هر $(i_1, \ldots, i_n) \in I$، $k_{i_1 \ldots i_n}$ یک عنصر ناصفر از K می‌باشد. فرض کنیم c عدد صحیح مثبتی بزرگتر از هر مولفهٔ i_s از هر عنصر $(i_1, \ldots, i_n)$ از I باشد. هرگاه $(i_1, \ldots, i_n), (j_1, \ldots, j_n) \in I$ چنان باشند که

$$i_1 + ci_2 + c^2 i_3 + \cdots + c^{n-1} i_n = j_1 + cj_2 + c^2 j_3 + \cdots + c^{n-1} j_n,$$

آنگاه $c \mid i_1 - j_1$ که‌ناممکن است مگر $i_1 = j_1$ (چون $c > i_1 \geq 0$ و $c > j_1 \geq 0$ ایجاب می‌کنند که $c > |i_1 - j_1|$). درنتیجه، $i_2 + ci_3 + \cdots + c^{n-2} i_n = j_2 + cj_3 + \cdots + c^{n-2} j_n$. مثل‌قبل، $c \mid i_2 - j_2$، که از آنجا $i_2 = j_2$. تکرار این استدلال نشان می‌دهد که $(i_1, \ldots, i_n) = (j_1, \ldots, j_n)$. بنابراین، مجموعهٔ

$$\{i_1 + ci_2 + c^2 i_3 + \cdots + c^{n-1} i_n \mid (i_1, \ldots, i_n) \in I\}$$

از $|I|$ عدد صحیح نامنفی متمایز تشکیل شده است؛ بخصوص، به‌ازای $(j_1, \ldots, j_n) \in I$ ی، این مجموعه دارای عنصر ماکزیمم **منحصر به فرد** $j_1 + cj_2 + \cdots + c^{n-1} j_n$ می‌باشد. فرض کنیم

$$v_2 = u_2 - u_1^c, v_3 = u_3 - u_1^{c^2}, \ldots, v_n = u_n - u_1^{c^{n-1}}.$$

اگر بستگی جبری فوق را پس از جانشانیهای $u_i = v_i + u_1^{c^{i-1}}$ $(2 \le i \le n)$ بسط دهیم، خواهیم داشت

$$k_{j_1 \dots j_n} u_1^{j_1 + cj_2 + c^2 j_3 + \dots + c^{n-1} j_n} + f(u_1, v_2, v_3, \dots, v_n) = 0,$$

که در آن درجهٔ $f \in K[x_1, \dots, x_n]$ نسبت به x_1 اکیدا" از $j_1 + cj_2 + \dots + c^{n-1} j_n$ کمتر است. بنابراین، u_1 ریشه‌ای از چندجمله‌ای تکین

$$x^{j_1 + cj_2 + \dots + c^{n-1} j_n} + k_{j_1 \dots j_n}^{-1} f(x, v_2, \dots, v_n) \in K[v_2, \dots, v_n][x]$$

می‌باشد. درنتیجه، u_1 روی $K[v_2, \dots, v_n]$ صحیح است. بنابر قضیهٔ ۵۰۵، $K[u_1, v_2, \dots, v_n] = K[v_2, \dots, v_n][u_1]$ روی $K[v_2, \dots, v_n]$ صحیح می‌باشد. چون هر u_i $(2 \le i \le n)$ بوضوح روی $K[u_1, v_2, \dots, v_n]$ صحیح است، قضایای ۵۰۵ و ۶۰۵ ایجاب می‌کنند که

$$R = K[u_1, \dots, u_n]$$

روی $K[v_2, \dots, v_n]$ صحیح می‌باشد (درنتیجه، F روی $K(v_2, \dots, v_n)$ جبری می‌باشد). هرگاه $\{v_2, \dots, v_n\}$ مستقل جبری باشد، آنگاه، طبق نتیجهٔ VI ۶۰۱۰، $r = n - 1$ و قضیه ثابت شده است. در غیر این صورت، استدلال پیشین با $K[v_2, \dots, v_n]$ به جای R نشان می‌دهد که، به‌ازای $w_3, \dots, w_n \in R$ ای، $K[v_2, \dots, v_n]$ روی $K[w_3, \dots, w_n]$ صحیح است. بنابر قضیهٔ ۶۰۵، R روی $K[w_3, \dots, w_n]$ صحیح است (که از آنجا F روی $K(w_3, \dots, w_n)$ جبری است و $r \le n - 2$). اگر $(w_3, \dots, w_n)$ مستقل جبری باشد، کار تمام است. درغیر این صورت، فرایند قبل را می‌توان تکرار کرد و با استدلالی استقرایی زیرمجموعهٔ مستقل جبری $\{z_{n-r+1}, \dots, z_n\}$ از r عنصر R را به دست آورد به‌طوری که R روی $K[z_{n-r+1}, \dots, z_n]$ صحیح باشد.

حال فرض می‌کنیم K میدان و F یک توسیع میدان به‌طور جبری بسته از K باشد. هرگاه ایده‌آل حقیقی I از $K[x_1, \dots, x_n]$ با تولید متناهی باشد، مثلا" $I = (g_1, \dots, g_k)$، آنگاه واریتهٔ مستوی $V(I)$ بوضوح مرکب از تمام عناصر $(a_1, \dots, a_n) \in F^n$ است که یک ریشهٔ مشترک $g_1, \dots, g_k$ می‌باشد (ر.ک. تمرین ۴). اگر $n = 1$، $K[x_1]$ یک دامنهٔ ایده‌آل اصلی است و واضح است که $V(I)$ ناتهی می‌باشد. به‌طور کلی (و تا حدی با تعجب) داریم:

لم ۳۰۷. هرگاه F یک توسیع میدان به‌طور جبری بسته از میدان K بوده و I یک

ایده‌آل حقیقی از $K[x_1, \ldots, x_n]$ *باشد، آنگاه واریتهٔ مستوی* $V(I)$ *تعریف شده به وسیلهٔ* I *در* F^n *ناتهی است.*

برهان. بنابر قضایای III ۱۸.۲۰ و III ۱۹.۲۰، I مشمول یک ایده‌آل اول حقیقی P است، که از آنجا $V(P) \subset V(I)$. درنتیجه، کافی است ثابت کنیم $V(P)$ به‌ازای هر ایده‌آل اول حقیقی P از $K[x_1, \ldots, x_n]$ ناتهی است. ملاحظه می‌کنیم که $P \cap K = 0$ (در غیر این صورت، $0 \neq a \in P \cap K$، که از آنجا $1_K = a^{-1}a \in P$، که با حقیقی بودن P تناقض دارد).

فرض کنیم R دامنهٔ صحیح $K[x_1, \ldots, x_n]/P$ بوده (ر.ک. قضیهٔ III ۱۶.۲۰) و $\pi : K[x_1, \ldots, x_n] \to R$ بروریختی کانونی باشد. هرگاه $\pi(x_i) \in R$ را با u_i نشان دهیم، آنگاه $R = \pi(K)[u_1, \ldots, u_n]$. به علاوه، چون $K \cap P = 0$، π، K را به‌طور یکریخت روی $\pi(K)$ می‌نگارد[1]؛ بخصوص، $\pi(K)$ یک میدان می‌باشد. بنابر لم نرمال‌سازی نوتر، زیرمجموعهٔ $\{t_1, \ldots, t_r\}$ از R وجوددارد به‌طوری که $\{t_1, \ldots, t_r\}$ روی $\pi(K)$ مستقل جبری بوده و R روی $S = \pi(K)[t_1, \ldots, t_r]$ صحیح است. هرگاه M ایده‌آل S تولیدشده به‌وسیلهٔ $t_1, \ldots, t_r$ باشد، آنگاه نگاشت $\pi(K) \to S/M$ داده شده با $\pi(a) \mapsto \pi(a) + M$ یکریختی است (ر.ک. قضیهٔ VI ۲.۱۰). درنتیجه، بنابر قضیهٔ III ۲۰.۲۰، M یک ایده‌آل ماکزیمال S می‌باشد. بنابراین، یک ایده‌آل ماکزیمال مانند N از R وجود دارد به‌طوری که $N \cap S = M$ (قضایای ۹.۵ و ۱۲.۵). فرض کنیم $\tau : R \to R/N$ بروریختی کانونی باشد. بنابر قضیهٔ III ۲۰.۲۰، $\tau(R) = R/N$ میدان‌است. حال قضیهٔ دوم یکریختی III ۱۲.۲۰ همراه با نگاشتهای تعریف شده در بالا یکریختی زیر را به دست می‌دهد:

$$K \cong \pi(K) \cong S/M = S/(N \cap S) \cong (S + N)/N = \tau(S),$$

که با $a \mapsto \pi(a) \mapsto \pi(a) + M \mapsto \pi(a) + N = \tau(\pi(a))$ داده‌شده است. فرض کنیم $\overline{\tau(R)}$ یک بسط جبری از $\tau(R)$ باشد. چون R روی S صحیح است، $\tau(R)$ یک توسیع میدان جبری از $\tau(S)$ است؛ درنتیجه، $\overline{\tau(R)}$ نیز یک بسط جبری $\tau(S)$ می‌باشد (قضیهٔ V ۴.۳۰). اما F شامل یک بسط جبری مانند $\bar{K}$ از K است (تمرین V ۷.۳۰). بنابر قضیهٔ V ۸.۳۰، یکریختی $K \cong \tau(S)$ به‌یک‌یکریختی‌مانند $\bar{K} \cong \overline{\tau(R)}$ توسیع می‌یابد. تحدید معکوس این یکریختی تکریختی $\sigma : \tau(R) \to \bar{K} \subset F$ را به دست می‌دهد. فرض کنید ϕ ترکیب $K[x_1, \ldots, x_n] \xrightarrow{\pi} R \xrightarrow{\tau} \tau(R) \xrightarrow{\sigma} F$ بوده و تحقیق کنید که $\phi \mid K = 1_K$ و $\phi \mid P = 0$

1. Noether

درنتیجه، به‌ازای هر $f(x_1, \ldots, x_n) \in P \subset K[x_1, \ldots, x_n]$،

$$f(\phi(x_1), \ldots, \phi(x_n)) = \phi(f(x_1, \ldots, x_n)) = 0,$$

که از آنجا $(\phi(x_1), \ldots, \phi(x_n))$ یک‌صفر P در F^n می‌باشد. بنابراین، $V(P)$ ناتهی خواهد بود.

حکم ۴۰۷ (قضیهٔ صفرهای هیلبرت). *فرض کنیم F یک توسیع میدان به طور جبری بسته از میدان K بوده و I یک ایده‌آل حقیقی از $K[x_1, \ldots, x_n]$ باشد. همچنین، به‌ازای هر $g \in I$، $V(I) = \{(a_1, \ldots, a_n) \in F^n \mid g(a_1, \ldots, a_n) = 0$، دراین صورت،*

$$\begin{aligned} Rad\, I &= J(V(I)) \\ &= \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0,\ (a_1, \ldots, a_n) \in V(I) \text{ به‌ازای هر}\} \end{aligned}$$

به‌عبارت دیگر، به‌ازای هر صفر $(a_1, \ldots, a_n)$ از I در F^n، $f(a_1, \ldots, a_n) = 0$ اگر و فقط اگر به‌ازای $m \geq 1$ ی، $f^m \in I$.

تبصره. با استفاده از لم ۳۰۷ قضیه را ثابت می‌کنیم. چون قضیه لم را ایجاب می‌کند (تمرین ۶)، این دو عملاً باهم معادلند.

برهان ۴۰۷. هرگاه $f \in \text{Rad } I$، آنگاه‌به‌ازای $m \geq 1$ ی $f^m \in I$ (قضیهٔ ۶۰۲). هرگاه $(a_1, \ldots, a_n)$ صفری از I در F^n باشد، آنگاه $f^m(a_1, \ldots, a_n) = (f(a_1, \ldots, a_n))^m = 0$. درنتیجه، چون F میدان است، $f(a_1, \ldots, a_n) = 0$. بنابراین، $\text{Rad } I \subset JV(I)$.

به عکس، فرض کنیم $f \in JV(I)$. می‌توان فرض کرد $f \neq 0$، زیرا $0 \in \text{Rad } I$. $K[x_1, \ldots, x_n]$ را زیرحلقه‌ای از حلقهٔ $K[x_1, \ldots, x_n, y]$ ازچندجمله‌ایها با $n+1$ مجهول روی K می‌گیریم. فرض‌کنیم L ایده‌آل ناصفر $K[x_1, \ldots, x_n, y]$ باشد که به وسیلهٔ I و $yf - 1_F$ تولیدشده‌است. واضح است که هرگاه $(a_1, \ldots, a_n, b)$ صفری از L در F^{n+1} باشد، آنگاه $(a_1, \ldots, a_n)$ بایدصفری از I در F^n باشد. اما، به‌ازای هر صفر $(a_1, \ldots, a_n)$ از I در F^n،

$$(yf - 1_F)(a_1, \ldots, a_n, b) = bf(a_1, \ldots, a_n) - 1_F = -1_F$$

بنابراین، L صفری در F^{n+1} ندارد؛ یعنی، $V(L)$ تهی است. درنتیجه، بنابر لم ۳۰۷، $L = K[x_1, \ldots, x_n, y]$، که از آنجا $1_F \in L$. لذا،

$$1_F = \sum_{i=1}^{t-1} g_i f_i + g_t(yf - 1_F),$$

که در آن $f_i \in I$ $(1 \le i \le t-1)$ و $g_i \in K[x_1, \ldots, x_n, y]$، همریختی ارزیابی $K[x_1, \ldots, x_n, y] \to K(x_1, \ldots, x_n)$ را با $x_i \mapsto x_i$ و $y \mapsto f^{-1} = 1_K/f(x_1, \ldots, x_n)$ تعریف می‌کنیم (نتیجهٔ III ۶.۵۰). پس در میدان $K(x_1, \ldots, x_n)$

$$1_F = \sum_{i=1}^{t-1} g_i(x_1, \ldots, x_n, f^{-1}) f_i(x_1, \ldots, x_n).$$

فرض‌کنیم m عدد صحیح مثبتی بزرگتر از درجهٔ g_i نسبت به y به‌ازای هر i $(1 \le i \le t-1)$ باشد. دراین‌صورت، به‌ازای هر i، $f^m(x_1, \ldots, x_n)g_i(x_1, \ldots, x_n, f^{-1})$ در $K[x_1, \ldots, x_n]$ قرار دارد، که از آنجا

$$f^m = f^m 1_F = \sum_{i=1}^{t-1} f^m(x_1, \ldots, x_n)g_i(x_1, \ldots, x_n, f^{-1}) f_i(x_1, \ldots, x_n) \in I.$$

بنابراین، $f \in \operatorname{Rad} I$؛ و درنتیجه، $J\mathcal{V}(I) \subset \operatorname{Rad} I$.

حال تعیین اشیاء بستهٔ مذکور در مقدمهٔ این بخش کار آسانی است (تمرینهای ۱ تا ۳).

این بخش را با تلاشی غیرصوری برای ایجاد رابطهٔ بین هندسه و جبر که روش کلاسیک پرداختن به هندسهٔ جبری را وصف می‌کند به پایان می‌بریم. فرض کنیم K یک میدان باشد. هر چندجمله‌ای $f \in K[x_1, \ldots, x_n]$ با جانشانی $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$ تابعی مانند $F: K^n \to K$ را معین می‌کند. اگر $V = V(I)$ یک واریتهٔ مستوی مشمول K^n باشد، تحدیداین تابع به V یک **تابع منتظم** بر V نامیده می‌شود. توابع منتظم $V \to K$ حلقه‌ای مانند $\Gamma(V)$ تشکیل می‌دهندکه با

$$K[x_1, \ldots, x_n]/J(V(I))$$

یکریخت است (تمرین ۱۰). این حلقه **حلقهٔ مختصات** V نام دارد. چون $I \subset J(V(I)) = \operatorname{Rad} I$، حلقهٔ $\Gamma(V)$ عنصرپوچ‌توان ناصفردارد. به علاوه، $\Gamma(V)$ یک جبر با تولید متناهی روی K است (زیرا $K[x_1, \ldots, x_n]$ و ایده‌آل $J(V(I))$ چنین‌اند؛ ر.ک. بخش IV ۷.۰). به عکس، می‌توان ثابت کرد که هر K ـ جبر با تولید متناهی بدون عنصر پوچ‌توان ناصفر حلقهٔ مختصات یک واریتهٔ مستوی است. بنابراین، تناظر یک به یکی بین واریته‌های مستوی و ردهٔ حلقه‌های تعویضپذیر نسبتاً " خاص موجود است. با تعریف مناسبی از

ریختها، واریته‌های مستوی، همانند حلقه‌های تعویضپذیر مورد بحث، یک رسته تشکیل می‌دهند و این تناظر عملا" یک "تعادل" رسته‌ها می‌باشـــــد. لذا، احکام مربوط به واریته‌های مستـوی معادل احکامی در باب جبر تعویضپذیر است. برای اطلاعات بیشتر، ر.ک. دبلیو. فولتون[1] [۵۳] و آی. جی. مک‌دونالد[2] [۵۵].

تمرینات

تذکر. F همواره یک توسیع میدان به‌طور جبری بسته از میدان K است؛ J ، V ، و F^n همانند در فوق هستند.

۱. زیـرمجمـوعهٔ Y از F^n بسته است (یعنی، $V(J(Y)) = Y$) اگر و فقط اگر Y یک K ــ واریتهٔ مستوی معین شده به وسیلهٔ زیرمجموعه‌ای مانند S از $K[x_1, \ldots, x_n]$ باشد.

۲. زیرمجموعهٔ S از $K[x_1, \ldots, x_n]$ بسته است (یعنی، $J(V(S)) = S$) اگر و فقط اگر S یک ایده‌آل رادیکال باشد (یعنی، S یک ایده‌آل بوده و $S = \mathrm{Rad}\, S$).

۳. یک تناظر یک به یک عکس کنندهٔ شمول بین مجموعهٔ K ــ واریته‌های مستوی در F^n و مجموعهٔ ایده‌آلهای رادیکال $K[x_1, \ldots, x_n]$ وجوددارد. [ر.ک. تمرینهای ۱ و ۲].

۴. هر K ــ واریتـهٔ مستـوی در F^n به شکل $V(S)$ است، که در آن S زیرمجموعه‌ای متناهی از $K[x_1, \ldots, x_n]$ می‌باشد. [**راهنمایی.** قضایای ۹.۱ و ۹.۴ و تمرین ۳.]

۵. هرگاه $V_1 \supset V_2 \supset \cdots$ یک‌زنجیرکاهشی‌از K ــ واریته‌هادر F^n باشد، آنگاه، به‌ازای m ی، $V_m = V_{m+1} = \cdots$. [**راهنمایی.** قضیهٔ ۹.۴ و تمرین ۳.]

۶. نشان دهید که قضیهٔ صفرها لم ۳.۷ را ایجاب می‌کند.

۷. هرگاه $I_1, \ldots, I_k$ ایده‌آلهایی از $K[x_1, \ldots, x_n]$ باشند، آنگاه

$$V(I_1 \cap I_2 \cap \cdots \cap I_k) = V(I_1) \cup V(I_2) \cup \cdots \cup V(I_k)$$

و $V(I_1 I_2 \cdots I_k) = V(I_1) \cap V(I_2) \cap \cdots \cap V(I_k)$.

۸. K ــ واریتهٔ V در F^n **تحویل‌ناپذیر** است مشروط براینکه هر وقت $V = W_1 \cup W_2$ و هر W_i یک K ــ واریته در F^n باشد، $V = W_1$ یا $V = W_2$.

---

1. W. Fulton 2. I. G. MacDonald

(آ) ثابت کنید V تحویل‌ناپذیر است اگر و فقط اگر $J(V)$ یک ایده‌آل اول در $K[x_1, \ldots, x_n]$ باشد.

(ب) فرض کنید $F = \mathbf{C}$ و $S = \{x_1^2 - 2x_2^2\}$. در این صورت، $V(S)$ به عنوان $\mathbf{Q}$ ــ واریته تحویل‌ناپذیر است ولی به عنوان $\mathbf{R}$ ــ واریته چنین نیست.

۹. هر K ــ واریتهٔ ناتهی در F^n را می‌توان به‌طور منحصر به فرد به صورت اجتماع متناهی $V_1 \cup V_2 \cup \cdots \cup V_k$ از K ــ واریته‌های مستوی در F^n نوشت به‌طوری که به‌ازای $i \neq j$، $V_i \not\subseteq V_j$ و هر V_i تحویل‌ناپذیر باشد (تمرین ۸).

۱۰. حلقهٔ مختصات یک K ــ واریتهٔ مستوی $V(I)$ با $K[x_1, \ldots, x_n]/J(V(I))$ یکریخت می‌باشد.

۹

ساختار حلقه‌ها

در قسمت اول این فصل، یک نظریهٔ ساختاری کلی برای حلقه‌ها عرضه می‌شود. با آنکه مفاهیم و تکنیکهای ارائه شده کاربردهای وسیعی دارند، قضایای ساختاری کامل فقط برای بعضی از رده‌های حلقه‌ها در دسترس است. روش اساسی تعیین یک چنین رده از حلقه‌ها را می‌توان شهودا "به صورت زیرتوصیف کرد. خاصیت "نامطلوب" P را درنظر می‌گیریم که در شرایطی صدق می‌کند؛ بخصوص، اینکه هر حلقه ایده‌آلی دارد که نسبت به داشتن خاصیت P ماکزیمال‌است. این ایده‌آل P ــ رادیکال حلقه نام دارد. سپس سعی می‌کنیم قضایای ساختاری ردهٔ حلقه‌ها با P ــ رادیکال صفر را بیابیم. اغلب باید با فرضهایی اضافی (نظیر شرایط زنجیری مناسب) قضایای ساختاری واقعا" قویتری به دست آورد. این ایده‌ها در مقدمهٔ بخشهای ۱ و ۲ زیر به‌طور مشروح مطرح خواهند شد. لازم است خواننده پیش از آغاز جدی فصل این دو بحث را بخواند.

دو رادیکال مختلف، رادیکال ژاکوبسون (بخش ۲) و رادیکال اول (بخش ۴)، را بررسی خواهیم کرد. در بخش ۳ قضایای ساختاری بسیار دقیق و مفیدی برای حلقه‌های نیمه سادهٔ آرتینی چپ (یعنی، حلقه‌های آرتینی چپ با رادیکال ژاکوبسون صفر) به دست می‌آوریم. قضیهٔ گولدی[1] در بخش ۴ مطرح می‌شود. این قضیه حلقه‌های نیمه‌اول نوتری چپ (یعنی، حلقه‌های نوتری چپ با رادیکال اول صفر) را توصیف می‌کند. سنگ زیرین تمام این قضایای ساختاری حلقه‌های درونریختی فضاهای برداری روی حلقه‌های بخشی و بعضی از زیرحلقه‌های "چگال" این حلقه‌ها می‌باشد (بخش ۱).

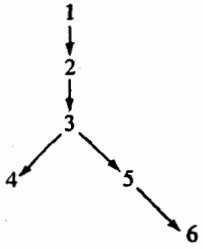
در دو بخش آخر فصل به جبرهای روی یک حلقهٔ تعویضپذیر یکدار می‌پردازیم.

1. Godie

رادیکال ژاکوبسون و مفاهیم و نتایج مربوطه به‌جبرها سرایت می‌یابند (بخش ۵) . جبرهای بخشی در بخش ۶ مطالعه خواهند شد .

روند کار در این فصل ارتباط نزدیک بین ساختار یک حلقه و ساختار مدولها روی حلقه است . استفاده از مدولها در بررسی حلقه‌ها به اطلاعاتی جدید و قضایایی عمیق منجر خواهد شد .

ارتباط بخشهای این فصل باهم به صورت زیر خواهد بود :



قسمت اعظم بحث ما به نتایج بخش VIII ۱۰ (شرایط زنجیری) وابسته است .

۱ حلقه‌های ساده و اولیه

در این بخش حلقه‌هایی مطالعه می‌شوند که سنگ زیرین نظریهٔ ساختاری حلقه‌ها قرار خواهند گرفت .

بحث را با یادآوری چند مطلب شروع می‌کنیم که بخش اعظمی از این فصل را موجب می‌شوند .

(یک) هرگاه V یک فضای برداری روی حلقهٔ بخشی D باشد ، آنگاه $\mathrm{Hom}_D(V,V)$ یک حلقه است (تمرین IV ۷.۱۰) ، که **حلقهٔ درونریختی** V نام دارد .

(دو) حلقهٔ درونریختی هر فضای برداری با بعد متناهی روی یک حلقهٔ بخشی با حلقهٔ تمام ماتریسهای $n \times n$ روی یک حلقهٔ بخشی (احتمالا " متفاوت) یکریخت است (قضیهٔ VII ۴.۱۰) .

(سه) هرگاه D یک حلقهٔ بخشی باشد ، آنگاه $\mathrm{Mat}_n D$ ساده بوده (یعنی ، ایده‌آل حقیقی ندارد ؛ تمرین III ۹.۲۰) و آرتینی چپ و راست است (نتیجهٔ VIII ۱۲.۱۰) . درنتیجه ، بنابر قسمت (دو) ، هر حلقهٔ درونریختی از یک فضای برداری با بعد متناهی روی یک حلقهٔ بخشی هم ساده است هم آرتینی .

(چهار) حلقهٔ درونریختی یک فضای برداری با بعد نامتناهی روی یک حلقهٔ بخشی نه ساده‌است نه آرتینی (تمرین ۳) . اما یک چنین حلقه به مفهوم تعریف شده در زیر اولیه است .

حلقه‌های ماتریسی و حلقه‌های درونریختی فضاهای برداری روی حلقه‌های بخشی در بسیاری از زمینه‌های مختلف به‌طور طبیعی ظاهر می‌شوند . این حلقه‌ها مفاهیم ریاضی بسیار مفیدی هستند . درنتیجه ، معقول به نظر می‌رسد که این حلقه‌ها ، یا دست‌کم حلقه‌هایی که شباهت زیادی به آنها دارند ، را مبنای یک نظریهٔ ساختاری گرفته و سعی کنیم حلقه‌های دلخواه را برحسب این حلقه‌های اساسی توصیف کنیم .

دو خاصیت اساسی حلقهٔ درونریختی فضای برداری V را درنظر می‌گیریم : سادگی (تعریف ۱۰۱) و اولیه بودن (تعریف ۵۰۱) . همانطورکه در بالا گفتیم ، این دو مفهوم تقریبا" نظیر حالاتی هستند که V با بعد متناهی یا نامتناهی است . در این بخش حلقه‌های ساده‌و اولیه را تحلیل کرده‌و نشان می‌دهیم که در چند حالت مهم با حلقه‌های درونریختی یکی هستند . در حالات دیگر ، به حد کافی به حلقه‌های درونریختی نزدیک خواهند شد .

به‌طور دقیقتر ، نشان می‌دهیم که حلقهٔ اولیهٔ دلخواه R با نوع خاصی زیرحلقه (به نام زیرحلقهٔ چگال) از حلقهٔ درونریختی فضای برداری V روی حلقهٔ بخشی D یکریخت است (قضیهٔ ۱۲۰۱) . R آرتینی چپ است اگر و فقط اگر $\dim_D V$ متناهی باشد (قضیهٔ ۹۰۱) . در این حالت کلاسیک ، حلقه‌های ساده و اولیه یکی شده و R عملا" با حلقهٔ درونریختی تام V یکریخت است (قضیهٔ ۱۴۰۱) . به‌علاوه ، در این وضع ، $\dim_D V$ به‌طور منحصر به فرد و V با تقریب یکریختی معین می‌شود (حکم ۱۷۰۱) . این نتایج اساسی بودن مفاهیم سادگی و اولیه بودن را بیش از پیش توجیه خواهند کرد .

همانطور که در مقدمهٔ این فصل گفتیم ، مدولها نقشی اساسی درنظریهٔ حلقه‌ها دارند . درنتیجه ، با تعریف و ارائهٔ خواص مقدماتی سادگی برای حلقه‌ها و مدولها شروع می‌کنیم .

تعریف ۱۰۱ . مدول (چپ) A روی حلقهٔ R *ساده* (یا *تحویل‌ناپذیر*) است مشروط بر اینکه $RA \neq 0$ و A زیرمدول حقیقی نداشته باشد . حلقهٔ R *ساده* است اگر $R^2 \neq 0$ و R ایده‌آل (دوطرفهٔ) حقیقی نداشته باشد .

چند تبصره. (یک) هر مدول [حلقهٔ] ساده ناصفر است. (دو) هر مدول ساده روی یک حلقهٔ یکداریکانی است (تمرین IV ۱۷۰۱۰). مدول یکانی A روی حلقهٔ یکدار R دارای خاصیت $RA \neq 0$ است؛ درنتیجه، A ساده‌است‌اگروفقط‌اگر A زیرمدول‌حقیقی نداشته باشد.

(سه) هر مدول سادهٔ A دوری است؛ درواقع، به‌ازای هر $a \in A$ ی ناصفر، $A = Ra$. [**برهان.** هر دوی Ra $(a \in A)$ و $B = \{c \in A \mid Rc = 0\}$ زیرمدول A اند؛ درنتیجه، بنابرسادگی، مساوی 0 یا A می‌باشند. اما $RA \neq 0$ ایجاب‌می‌کندکه $B \neq A$. درنتیجه، $B = 0$، که ازآنجابه‌ازای‌هر $a \in A$ ی ناصفر، $Ra = A$.] با اینحال، یک مدول دوری لزوما" ساده نیست (مثلا"، $\mathbf{Z}$ ــ مدول دوری Z_6).

(چهار) تعاریف "ساده" برای‌گروهها، مدولها، و حلقه‌ها را می‌توان در یک تعریف کلی آورد که تقریبا" به صورت زیر است: شئی جبری C که به مفهومی نابدیهی است (مثلا"، $RA \neq 0$ یا $R^2 \neq 0$) **ساده** می‌باشد اگر هر همریختی با دامنهٔ C دارای هستهٔ 0 یا C باشد. در اینجا نکته این است که عدم وجود هسته‌های نابدیهی معادل عدم وجود زیرگروههای نرمال‌حقیقی یک گروه یا زیرمدولهای حقیقی یک مدول یا ایده‌آلهای حقیقی یک حلقه، بسته به حالت، می‌باشد.

مثال. هر حلقهٔ بخشی یک‌حلقهٔ ساده و یک D ــ مدول ساده است (ر.ک. تبصره‌های پیش از قضیهٔ III ۲۰۲۰).

مثال. فرض کنیم D یک حلقهٔ بخشی بوده و $R = \mathrm{Mat}_n D$ $(n > 1)$. به‌ازای هر k $(1 \leq k \leq n)$، $I_k = \{(a_{ij}) \in R \mid a_{ij} = 0 \text{ ، } j \neq k$ به‌ازای $\}$ یک R ــ مدول چپ ساده است (ر.ک. برهان نتیجهٔ VIII ۱۲۰۱۰).

مثال. مثال فوق نشان می‌دهد که، اگر $n > 1$، $\mathrm{Mat}_n D$ (D یک حلقهٔ بخشی است) یک **مدول** چپ ساده روی خود نیست. اما، بنابر تمرین III ۹۰۲۰، **حلقهٔ** $\mathrm{Mat}_n D$ $(n \geq 1)$ ساده است. لذا، طبق قضیهٔ VII ۴۰۱۰، حلقهٔ درونریختی هر فضای برداری با بعد متناهی روی حلقهٔ بخشی یک حلقهٔ ساده می‌باشد.

مثال. گوییم ایده‌آل چپ I از حلقهٔ R یک ***ایده‌آل چپ مینیمال*** است اگر $I \neq 0$ و

به‌ازای هر ایده‌آل چپ J که $0 \subset J \subset I$ ، $J = 0$ یا $J = I$. ایده‌آل چپ I از R که $RI \neq 0$ یک R ــ مدول چپ ساده است اگر و فقط اگر I یک ایـــــــده‌آل چپ مینیمال باشد .

مثال . فرض کنیم F میدانی با مشخص صفر بوده و R گروه **جمعی** چندجمله‌ایهای $F[x,y]$ باشد . ضرب در R را با درنظرگرفتن پخشپذیری ، $xy = yx + 1$ ، و به‌ازای هر $a \in F$ ، $ax = xa, ay = ya$ تعریف می‌کنیم . دراین صورت ، R یک حلقهٔ ساده‌ٔ تعریف شده بوده و مقسوم‌علیه صفر ندارد و یک حلقهٔ بخشی **نمی‌باشد** (تمرین ۱) .

فرض کنیم $A = Ra$ یک R ــ مدول‌دوری باشد . نگاشت $\theta : R \to A$ تعریف شده با $r \mapsto ra$ یک بـــوریختی R ــ مدولهاست که هسته‌اش I یک ایده‌آل (زیرمدول) چپ R است (قضیهٔ IV ۵.۱۰) . بنابر قضیهٔ اول یکریختی IV ۷.۱۰ ، R/I با A یکریخت است . بنـابر قضیهٔ IV ۱۰.۱۰ ، هر زیرمدول R/I به شکل J/I است ، که در آن J یک ایده‌آل چپ R شامل I می‌باشد . درنتیجه ، R/I (و لـــذا ، A) زیرمدول حقیقی ندارد اگر و فقط اگر I یک ایده‌آل چپ ماکزیمال R باشد . چون بنابر تبصرهٔ (سه) فوق هر R ــ مدول ساده‌دوری است ، هر R ــ مدول ساده به‌ازای ایده‌آل چپ ماکزیمالی چون I با R/I یکریخت‌است . به‌عکس ، اگر I ایده‌آل چپ ماکزیمالی از R باشد ، R/I ساده است مشروط بر اینکه $R(R/I) \neq 0$. شرط تضمین‌کنندهٔ $R(R/I) \neq 0$ در تعریف‌زیر داده می‌شود .

تعریف ۲.۱ . ایـــده‌آل چـــپ I در حلقهٔ R ***منتظم*** (یا **مدولی**) است اگر $e \in R$ ای موجود بـــاشد به‌طوری که به‌ازای هر $r \in R$ ، $r - re \in I$. به همین نحو ، ایده‌آل راست J ***منتظم*** است اگر $e \in R$ ای موجود باشد به‌طوری‌که به‌ازای هر $r \in R$ ، $r - er \in J$.

تبصره . هر ایده‌آل چپ در حلقهٔ یکدار R منتظم است (فرض کنید $e = 1_R$) .

قضیهٔ ۳.۱ . ***مدول چپ A روی حلقهٔ R ساده است اگر و فقط اگر A به‌ازای ایده‌آل چپ ماکزیمال منتظمی مانند I با R/I یکریخت باشد .***

چند تبصره. اگر R یکدار باشد، قضیه نتیجهٔ فوری بحث فوق است. قضیه در صورت تعویض همه جایی "چپ" با "راست" درست است.

برهان ۳۰۱. بحث پیش از تعریف ۲۰۱ نشان می‌دهد که هرگاه A ساده باشد، آنگاه $A = Ra \cong R/I$، که در آن ایده‌آل چپ ماکزیمال I هستهٔ θ است. چون $A = Ra$، به‌ازای $e \in R$ ای، $a = ea$. درنتیجه، به‌ازای هر $r \in R$، $ra = rea$ یا $(r - re)a = 0$، که از آنجا $r - re \in \operatorname{Ker}\theta = I$. بنابراین، I منتظم می‌باشد.

به عکس، فرض کنیم I یک ایده‌آل چپ ماکزیمال منتظم R باشد به‌طوری که $A \cong R/I$. در پرتو بحث پیش از تعریف ۲۰۱، کافی است ثابت شود که $R(R/I) \neq 0$. اگر چنین نباشد، به‌ازای هر $r \in R$، $r(e + I) = I$، که از آنجا $re \in I$. چون $r - re \in I$، داریم $r \in I$. لذا، $R = I$، که با ماکزیمالی I متناقض می‌باشد.

حال کـه نـکات لازم در باب سادگی را به دست آورده‌ایم به مفهوم اولیه بودن می‌پردازیم. برای تعریف حلقه‌های اولیه به قضیهٔ زیر نیاز داریم.

قضیهٔ ۴۰۱. *فرض کنیم B زیرمجموعه‌ای از مدول‌چپ A روی حلقهٔ R باشد. در این صورت، به ازای هر $b \in B$، $\alpha(B) = \{r \in R \mid rb = 0\}$ یک ایده‌آل چپ R است. هرگاه B زیر مدول A باشد، آنگاه $\alpha(B)$ یک ایده‌آل می‌باشد.*

$\alpha(B)$ *صفرساز (چپ)* B نام دارد. صفرساز راست یک مدول راست به همین نحو تعریف می‌شود.

طرح برهان ۴۰۱. به‌آسانی تحقیق می‌شود که $\alpha(B)$ یک ایده‌آل چپ است. فرض کنیم B یـک زیـرمـدول بـاشـد. هـرگاه $r \in R$ و $s \in \alpha(B)$، آنـگاه، به‌ازای هـر $b \in B$، $(sr)b = s(rb) = 0$، زیرا $rb \in B$. درنتیجه، $sr \in \alpha(B)$، که از آنجا $\alpha(B)$ یک ایده‌آل راست نیز می‌باشد.

تعریف ۵۰۱. مدول (چپ) A ***وفادار*** راست اگر صفرساز (چپ) آن $\alpha(A)$ مساوی 0 باشد.

حلقهٔ R ***اولیهٔ (چپ)*** است اگر یک R ــ مدول چپ وفادار ساده وجود داشته باشد.

حلقه‌های‌اولیهٔ راست به همین نحو تعریف می‌شوند. حلقه‌های اولیهٔ راستی وجود دارند که اولیهٔ چپ نیستند (ر.ک. جی. برگمن[1] [۵۸]). از حالا به بعد "اولیه" همیشه‌به‌معنی "اولیهٔ چپ" می‌باشد. با اینحال، تمام نتایج ثابت شده در موردحلقه‌های اولیهٔ چپ ***نعل به نعل*** در مورد حلقه‌های اولیهٔ راست برقرارند.

مثال. فرض کنیم V یک‌فضای برداری (احتمالا "با بعد نامتناهی) روی حلقهٔ بخشی D بوده و R حلقهٔ درونریختی $\mathrm{Hom}_D(V,V)$ از V باشد. به‌یاد آورید که V یک R ــ مدول چپ است که به‌ازای $v\in V, \theta\in R$ ، $\theta v = \theta(v)$ (تمرین IV ۷.۱۰). هرگاه u یک بردار ناصفر در V باشد، آنگاه پایه‌ای از V شامل u وجود دارد (قضیهٔ IV ۴.۲۰). هرگاه $v\in V$، آنگاه $\theta_v\in R$ ای وجوددارد‌به‌طوری که $\theta_v u = v$ (کافی‌است تعریف کنیم $\theta_v(u) = v$ و، به‌ازای‌سایرعناصرپایه‌مانند w ، $\theta_v(w) = 0$؛ دراین‌صورت، طبق قضایای IV ۲.۱۰ و IV ۲.۴۰ ، $\theta_v\in R$). بنابراین، به‌ازای هر $u\in V$ ی ناصفر، $Ru = V$؛ درنتیجه، V ، R ــ زیرمدول حقیقی ندارد. چون R یکدار است، $RV \neq 0$. لذا، V یک R ــ مدول ساده می‌باشد. هرگاه $\theta V = 0\ (\theta\in R)$ ، آنگاه واضح است که $\theta = 0$ ، که از آنجا $\mathrm{Ann}(V) = 0$ و V یک R ــ مدول وفاداراست. بنابراین، R اولیه می‌باشد. هرگاه V با بعدمتناهی روی D باشد، آنگاه، بنابر تمرین III ۹.۲۰ و قضیهٔ VII ۴.۱۰ ، R ساده می‌باشد. اماهرگاه V بابعدنامتناهی‌روی D باشد، آنگاه R ساده نخواهد بود: مجموعهٔ تمام $\theta\in R$ هایی که $\mathrm{Im}\,\theta$ زیرفضایی از V با بعد متناهی است یک ایده‌آل حقیقی R می‌باشد (تمرین ۳).

دو نتیجهٔ زیر مثالهای دیگری از حلقه‌های اولیه به دست خواهند داد.

حکم ۶.۱. ***حلقهٔ سادهٔ یکدار R اولیه می‌باشد.***

برهان. بنابر قضیهٔ III ۱۸.۲۰ ، R شامل ایده‌آل چپ ماکزیمال I است. چون R

1. G. Bergman

یکدار است، I منتظم است؛ درنتیجه، بنابر قضیهٔ ۳۰۱، R/I یک R ــ مدول ساده می‌باشد. چون $\mathcal{Q}(R/I)$ یک‌ایده‌آل R است که شامل 1_R نیست، بنابرسادگی $\mathcal{Q}(R/I) = 0$ بنابراین، R/I وفادار می‌باشد.

حکم ۷۰۱. حلقهٔ تعویضپذیر R *اولیه است اگر و فقط اگر* R میدان باشد.

برهان. بنابرحکم ۶۰۱، یک‌میدان اولیه است. به عکس، فرض کنیم A یک R ــ مدول چپ سادهٔ وفادار باشد. در این صورت، به‌ازای ایده‌آل چپ ماکزیمال منتظمی چون I از R، $A \cong R/I$. چون R تعویضپذیر است، I عملاً "یک ایده‌آل سوده و $I \subset \mathcal{Q}(R/I) = \mathcal{Q}(A) = 0$. و چون $I = 0$ منتظم است، عنصری چون $e \in R$ وجود دارد به‌طوری که به‌ازای هر $r \in R$، $r = re\ (=er)$. لذا، R حلقه‌ای تعویضپذیر و یکدار می‌باشد. چون $I = 0$ ماکزیمال است، بنابر نتیجهٔ ۲۱۰۲۰ III، R میدان می‌باشد.

برای توصیف حلقه‌های اولیهٔ تعویض‌ناپذیر، به مفهوم چگالی نیاز خواهیم داشت.

تعریف ۸۰۱. فرض کنیم V یک فضای برداری (چپ) روی حلقهٔ بخشی D باشد. زیرحلقهٔ R ازحلقهٔ درونریختی $Hom_D(V,V)$ یک **حلقهٔ *چگال از درونریختیهای* V** (یا یک **زیرحلقهٔ *چگال*** $Hom_D(V,V)$) نام دارد اگر به‌ازای هر عدد صحیح مثبت n، هر زیرمجموعهٔ مستقل خطی $\{u_1, \ldots, u_n\}$ از V، و هر زیرمجموعهٔ دلخواه $\{v_1, \ldots, v_n\}$ از V، $\theta \in R$ ای موجود باشد به‌طوری که $\theta(u_i) = v_i$ $(i = 1,2, \ldots, n)$.

مثال. $Hom_D(V,V)$ یک زیرحلقهٔ چگال خود است. زیرا هرگاه $\{u_1, \ldots, u_n\}$ یک زیرمجموعهٔ مستقل‌خطی از V باشد، آنگاه، بنابر قضیهٔ ۴۰۲۰ IV، پایه‌ای چون U از V وجود دارد که شامل $u_1, \ldots, u_n$ می‌باشد. هرگاه $v_1, \ldots, v_n \in V$، آنگاه، بنابر قضایای ۱۰۲۰ IV و ۴۰۲۰ IV، نگاشت $\theta : V \to V$ تعریف شده با $\theta(u_i) = v_i$ و $\theta(u) = 0$ به‌ازای $u \in U - \{u_1, \ldots, u_n\}$ یک عنصر تعریف شده‌ای از $Hom_D(V,V)$ است. همانطور که در قضیهٔ زیر می‌بینیم، در حالت بعد متناهی، $Hom_D(V,V)$ تنها زیرحلقهٔ چگال می‌باشد.

قضیهٔ ۹.۱ . *فرض کنیم* R *یک حلقهٔ چگال از درونریختیهای فضای برداری* V *روی حلقهٔ بخشی* D *باشد. در این صورت،* R *آرتینی چپ [راست] است اگر و فقط اگر* $\dim_D V$ *متناهی باشد، که در این صورت* $R = Hom_D(V,V)$.

برهان. هرگاه R آرتینی چپ بوده و $\dim_D V$ نامتناهی باشد، آنگاه یک زیرمجموعهٔ مستقل خطی نامتناهی مانند $\{u_1,u_2,\dots\}$ از V وجود دارد. بنابر تمرین IV ۷.۱۰، V یک $\mathrm{Hom}_D(V,V)$ ــ مدول چپ، و درنتیجه، یک R ــ مدول چپ، است. به‌ازای هر n، I_n را یک صفرساز چپ مجموعهٔ $\{u_1,\dots,u_n\}$ در R می‌گیریم. بنابر قضیهٔ ۴.۱، $I_1 \supset I_2 \supset \cdots$ یک زنجیرکاهشی از ایده‌آلهای چپ R است. فرض کنیم w عنصر ناصفری از V باشد. چون $\{u_1,\dots,u_{n+1}\}$ به‌ازای هر n مستقل خطی بوده و R چگال است، $\theta \in R$ ای وجود دارد به‌طوری که

$$\theta u_{n+1} = w \neq 0 \quad \text{و} \quad \theta u_i = 0 \ , \ i = 1,2,\dots,n$$ به‌ازای .

درنتیجه، $\theta \in I_n$ ولی $\theta \notin I_{n+1}$. بنابراین، $I_1 \supsetneq I_2 \supsetneq \cdots$ یک زنجیر حقیقتا" کاهشی است، که یک تناقض است. از اینرو، $\dim_D V$ متناهی می‌باشد.

به عکس، هرگاه $\dim_D V$ متناهی باشد، آنگاه V دارای پایهٔ متناهی $\{v_1,\dots,v_m\}$ است. هرگاه f عنصری از باشد، آنگاه، بنابر قضایای IV ۱.۲۰ و IV ۴.۲۰، f با عملش بر $v_1,\dots,v_m$ کاملا" معین است. چون R چگال است، $\theta \in R$ ای هست به‌طوری که

$$\theta(v_i) = f(v_i) \ , \ i = 1,2,\dots,m$$ به‌ازای ،

که از آنجا $f = \theta \in R$. بنابراین، $\mathrm{Hom}_D(V,V) = R$. اما، طبق قضیهٔ IV ۴.۱۰ و نتیجهٔ VIII ۱۲.۱۰، $\mathrm{Hom}_D(V,V)$ آرتینی می‌باشد.

برای اثبات اینکه یک حلقهٔ اولیهٔ دلخواه با حلقهٔ چگالی از درونریختیهای یک فضای برداری مناسب یکریخت است، به دو لم زیر نیاز خواهیم داشت.

لم ۱۰.۱ (شور[1]). *فرض کنیم* A *مدول ساده‌ای روی حلقهٔ* R *بوده و* B *یک* R ــ *مدول*

---

1. *Schur*

باشد.

(یک) هر همریختی $f : A \to B$ از R ـ مدولهای ناصفر یک تکریختی است؛

(دو) هر همریختی $g : B \to A$ از R ـ مدولهای ناصفر یک برووریختی است؛

(سه) حلقهٔ درونریختی $D = Hom_R(A,A)$ یک حلقهٔ بخشی است.

برهان. (یک) $\operatorname{Ker} f$ زیرمدولی از A است و $\operatorname{Ker} f \neq A$، زیرا $f \neq 0$. بنابراین، طبق سادگی، $\operatorname{Ker} f = 0$. (دو) $\operatorname{Im} g$ یک زیرمدول ناصفر A است، زیرا $g \neq 0$، که از آنجا، طبق سادگی، $\operatorname{Im} g = A$. (سه) هرگاه $h \in D$ و $h \neq 0$، آنگاه h طبق (یک) و (دو) یکریختی است. لذا، f معکوس دوطرفهٔ $f^{-1} \in \operatorname{Hom}_R(A,A) = D$ دارد (ر.ک. بند بعد ازتعریف IV ۲.۱۰). درنتیجه، هرعنصرناصفر D یک یکه است؛ لذا، D یک حلقهٔ بخشی می‌باشد.

تبصره. هرگاه A یک R ـ مدول ساده باشد، آنگاه A فضایی برداری روی حلقهٔ بخشی $\operatorname{Hom}_R(A,A)$ است که $fa = f(a)$ (تمرین IV ۷.۱۰ و لم ۱۰.۱).

لم ۱۱.۱. *فرض کنیم A یک‌مدول ساده روی حلقهٔ R باشد. A را یک فضای برداری روی حلقهٔ بخشی $D = Hom_R(A,A)$ می‌گیریم. هرگاه V یک D ـ زیرفضای با بعدمتناهی از D ـ فضای برداری A بوده و $a \in A - V$، آنگاه $r \in R$ ی وجود دارد به‌طوری که $ra \neq 0$ و $rV = 0$.*

برهان. اثبات به‌استقرابر $n = \dim_D V$ است. هرگاه $n = 0$، آنگاه $V = 0$ و $a \neq 0$. چون A ساده است، بنابر تبصرهٔ (سه) بعد از تعریف ۱۰.۱، $A = Ra$. درنتیجه، $r \in R$ ی وجوددارد به‌طوری‌که $ra = a \neq 0$ و $rV = r0 = 0$. فرض‌کنیم $\dim_D V = n > 0$ و قضیه برای ابعاد کمتر از n درست باشد. فرض کنیم $\{u_1, \ldots, u_{n-1}, u\}$ یک D ـ پایهٔ V بوده و W، D ـ زیرفضای $(n-1)$ بعدی پیموده شده‌به وسیلهٔ $\{u_1, \ldots, u_{n-1}\}$ باشد (اگر $n = 1$، $W = 0$). در این صورت، $V = W \oplus Du$ (فضای برداری مجموع مستقیم). W ممکن است یک R ـ زیرمدول A نباشد، ولی در هر حال، طبق قضیهٔ ۴.۱، صفرساز چپ $I = \mathfrak{a}(W)$ در R از W یک ایده‌آل چپ R است. درنتیجه، Iu یک R ـ زیرمدول

A است (تمرین IV ۳۰۱۰) . چون $u \in A - W$ ، فرض استقرا ایجاب می‌کند که $r \in R$ ی موجود باشد به‌طوری که $ru \neq 0$ و $rW = 0$ (یعنی ، $r \in I = \mathfrak{A}(W)$) . در نتیجه ، $0 \neq ru \in Iu$ ، که از آنجا $Iu \neq 0$. بنابراین ، طبق سادگی ، $A = Iu$.

[**تذکر .** عکس نقیض استدلال استقرایی به‌کار رفته در فوق نشان می‌دهد که هرگاه $v \in A$ و به‌ازای هر $r \in I$ ، $rv = 0$ ، آنگاه $v \in W$.]

باید $r \in R$ ی یافت بـه‌طوری که $ra \neq 0$ و $rV = 0$. هرگاه این r موجود نباشد ، آنگاه می‌توان نگاشتی مانند $\theta : A \to A$ به صـورت زیر تعریف کرد . به‌ازای $ru \in Iu = A$ ، قرار می‌دهیم $\theta(ru) = ra \in A$. حکـم می‌کنیم که θ تعریف شده است . هرگاه $r_1u = r_2u$ $(r_i \in I = \mathfrak{A}(W))$ ، آنگاه $(r_1 - r_2)u = 0$ ، که از آنجا

$$(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = 0.$$

درنتیجه ، طبق فرض ، $(r_1 - r_2)a = 0$. بنابراین ، $\theta(r_1u) = r_1a = r_2a = \theta(r_2u)$. تحقیق کنید که $\theta \in \mathrm{Hom}_R(A,A) = D$. پس ، به‌ازای هر $r \in I$ ،

$$0 = \theta(ru) - ra = r\theta(u) - ra = r(\theta(u) - a).$$

بنابراین ، طبق تذکر داخل کروشه در بالا ، $\theta(u) - a \in W$. درنتیجه ،

$$a = \theta u - (\theta u - a) \in Du + W = V,$$

که $a \notin V$ را نقض خواهد کرد . بنابراین ، $r \in R$ ی هست به‌طوری که $ra \neq 0$ و $rV = 0$.

قضیهٔ ۱۲۰۱ . (قضیهٔ چگالی ژاکوبسون) . *فـرض‌کنیـم R یک حلقهٔ اولیه و A یک R ــ مدول سادهٔ وفادار باشد . A را یک‌فضای‌برداری‌روی حلقهٔ بخشی $Hom_R(A,A) = D$ می‌گیریم . در ایـن صورت ، R با حلقهٔ چگالی‌از درونریختیهای D ــ فضای برداری A یکریخت است .*

تبصره . عکس قضیهٔ ۱۲۰۱ نیز ، درواقع به شکلی قویتر ، درست است (تمرین ۴) .

برهان ۱۲۰۱ . به آسانی معلوم می‌شود که‌نگاشت $\alpha_r : A \to A$ داده‌شده‌با $\alpha_r(u) = ru$ ، بـه‌ازای هـر $r \in R$ ، یک D ــ درونریختی A است ؛ یعنی ، $\alpha_r \in \mathrm{Hom}_D(A,A)$. به علاوه ، به‌ازای هر $r,s \in R$ ،

$$\alpha_{rs} = \alpha_r\alpha_s \quad \text{و} \quad \alpha_{(r+s)} = \alpha_r + \alpha_s .$$

درنتیجه، نگاشت $\alpha : R \to \mathrm{Hom}_D(A,A)$ تعریف‌شده‌با $\alpha(r) = \alpha_r$ همریختی‌تعریف شده‌ای از حلقه‌هاست. چون A یک R ــ مدول وفادار است، $\alpha_r = 0$ اگر و فقط $r \in \mathfrak{A}(A) = 0$. بنابراین، α تکریختی است؛ درنتیجه، R با زیرحلقهٔ $\mathrm{Im}\,\alpha$ از $\mathrm{Hom}_D(A,A)$ یکریخت است.

برای تکمیل بـرهان باید نشان دهیم که $\mathrm{Im}\,\alpha$ یک زیرحلقهٔ چگال $\mathrm{Hom}_D(A,A)$ است. بـه‌ازای زیـرمجموعهٔ D ــ مستقل خطی $U = \{u_1, \ldots, u_n\}$ از A و زیر مجموعهٔ دلخواه $\{v_1, \ldots, v_n\}$ از A، باید $\alpha_r \in \mathrm{Im}\,\alpha$ را طـوری یافت که بـه‌ازای $i = 1,2, \ldots, n$، $\alpha_r(u_i) = v_i$. بـه‌ازای هـر i، فرض کنیم V_i، D ــ زیـرفضای A باشد که به وسیلهٔ $\{u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n\}$ پیموده‌می‌شود. چون U، D ــ مستقل خطی است، $u_i \notin V_i$. درنتیجه، طبق لم ۱۱۰۱، $r_i \in R$ ی وجود دارد بـه‌طوری که $r_i u_i \neq 0$ و $r_i V_i = 0$. حال لم ۱۱۰۱ را بر زیرفضای صفر و عنصر ناصفر $r_i u_i$ اعمال می‌کنیم: $s_i \in R$ ی وجود دارد بـه‌طوری که $s_i r_i u_i \neq 0$ و $s_i 0 = 0$. چون $s_i r_i u_i \neq 0$، R ــ زیرمدول $Rr_i u_i$ از A ناصفراست، که از آنجا، به خاطر سادگی، $Rr_i u_i = A$. بنابراین، $t_i \in R$ ی وجـود دارد بـه‌طوری که $t_i r_i u_i = v_i$. فرض کنیم

$$r = t_1 r_1 + t_2 r_2 + \cdots + t_n r_n \in R.$$

به یاد آورید که بـه‌ازای $i \neq j$، $u_i \in V_j$، کهازآنجا $t_j r_j u_i \in t_j(r_j V_j) = t_j 0 = 0$. درنتیجه، بـه‌ازای هر $i = 1,2, \ldots, n$،

$$\alpha_r(u_i) = (t_1 r_1 + \cdots + t_n r_n)u_i = t_i r_i u_i = v_i.$$

بنابراین، $\mathrm{Im}\,\alpha$ یک حلقهٔ چگال از درونریختیهای D ــ فضای برداری A می‌باشد.

تبصره. تنها جایی که در برهان قضیهٔ ۱۲۰۱ از وفاداری A استفاده می‌شود در اثبات تکریختی α است. درنتیجه، برهان نشان می‌دهد که هر حلقه که مدول ساده‌ای چون A داشته‌باشد نقش همریختی دارد که یک حلقهٔ چگال از درونریختیهای D ــ فضای برداری A می‌باشد.

نتیجهٔ ۱۳۰۱. هرگاه R یک‌حلقهٔ اولیه باشد، آنگاه، به‌ازای یک حلقهٔ بخشی مانند D، یا R با حلقهٔ درونریختی یک فضای برداری با بعد متناهی روی D یکریخت است یا، به‌ازای هرعدد صحیح مثبت m، زیرحلقه‌ای‌مانند R_m از R و یک بروریختی حلقه‌ها

مانند $R_m \to Hom_D(V_m,V_m)$ وجوددارند ،که V_m یک‌فضای‌برداری m بعدی روی حلقهٔ D است .

تبصره . نتیجه را می‌توان بـرحسب حلقه‌های ماتریسی روی یک حلقهٔ بخشی از طریق قضیهٔ VII ۴.۱۰ نیز بیان کرد .

طرح برهان ۱۳.۱ . با نمادهای قضیهٔ ۱۲.۱ ،

$$\alpha : R \to \mathrm{Hom}_D(A,A)$$

یک تکـریختی اسـت به‌طوری که $R = \mathrm{Im}\ \alpha$ و $\mathrm{Im}\ \alpha$ در $\mathrm{Hom}_D(A,A)$ چگال‌است . هرگاه $\dim_D A = n$ متناهی‌باشد ،آنگاه ، طبق قضیهٔ ۹.۱ ، $\mathrm{Im}\ \alpha = \mathrm{Hom}_D(A,A)$. اگر $\dim_D A$ نـامتنـاهی بوده و $\{u_1,u_2,\ldots\}$ یک مجمـوعـهٔ مستقـل خطـی نامتناهی باشد ، V_m را D ــ زیرفضای m بعدی A می‌گیـریم که به وسیلهٔ $\{u_1,\ldots,u_m\}$ پیموده می‌شود . تحقیق کنید که $R_m = \{r \in R \mid rV_m \subset V_m\}$ زیـرحلقـه‌ای از R است . بـا استفاده از چگال بودن $R \cong \mathrm{Im}\ \alpha$ در $\mathrm{Hom}_D(A,A)$ ، نشان دهید که نگاشت $R_m \to \mathrm{Hom}_D(V_m,V_m)$ داده شده با $r \mapsto \alpha_r \mid V_m$ یک برووریختی تعریف شـده از حلقه‌هاست .

قضیهٔ ۱۴.۱ (ودربورن ــ آرتین) . *شرایط زیربرحلقهٔ آرتینی‌چپ* R *باهم معادلند :*

(یک) R *ساده است ؛*

(دو) R *اولیه است ؛*

(سه) R *با حلقهٔ درونریختی‌یک‌فضای‌برداری‌با بعد متناهی ناصفر مانند* V *روی حلقهٔ بخشی* D *یکریخت می‌باشد .*

(چهار) به‌ازای عدد صحیح مثبتی چون n ، R *با حلقهٔ تمام ماتریسهای* $n \times n$ *روی یک حلقهٔ بخشی یکریخت است .*

برهان . (دو) $\Rightarrow$ (یک) ابتدا مـلاحظه می‌کنیم که $I = \{r \in R \mid Rr = 0\}$ یک ایده‌آل R است ، کـه از آنجـا $I = R$ یا $I = 0$. چون $R^2 \neq 0$ ، بایدداشته باشیم $I = 0$.

چون R آرتینی چپ است، مجموعهٔ تمام ایده‌آلهای چپ ناصفر R شامل ایده‌آل چپ مینیمالی چون J می‌باشد. J ، R ـ زیر مدول حقیقی ندارد (R ـ زیرمدول J ایده‌آل چپ R است). حکم می‌کنیم که صفرساز $\mathcal{A}(J)$ از J در R صفر است. در غیر این صورت، طبق سادگی، $\mathcal{A}(J) = R$ و، به‌ازای هر $u \in J$ ی ناصفر، $Ru = 0$. درنتیجه، هر چنین u ی ناصفر مشمول $I = 0$ می‌باشد، که یک تناقض است. بنابراین، $\mathcal{A}(J) = 0$ و $RJ \neq 0$. لذا، J یک R ـ مدول سادهٔ وفادار است، که از آنجا R اولیه می‌باشد.

(سه) $\Rightarrow$ (دو) بنابر قضیهٔ ۱۲۰۱، R با حلقهٔ چگال T از درونریختیهای فضای برداری V روی حلقهٔ بخشی D یکریخت است. چون R آرتینی چپ است، بنابر قضیهٔ ۹۰۱، $R \cong T = \mathrm{Hom}_D(V,V)$.

(چهار) $\Leftrightarrow$ (سه) قضیهٔ VII ۴۰۱۰.

(یک) $\Rightarrow$ (چهار) تمرین III ۹۰۲۰.

این بخش را با اثبات اینکه به‌ازای حلقهٔ آرتینی چپ سادهٔ R اعداد صحیح، $\dim_D V$ و n در قضیهٔ ۱۴۰۱ به‌طور منحصر به فرد تعیین می‌شوند و حلقه‌های بخشی در قضیهٔ ۱۴۰۱ (سه) و (چهار) با تقریب یکریختی معین است به پایان می‌بریم. در این راه به دو لم نیاز داریم.

لم ۱۵۰۱. *فرض کنیم V یک فضای برداری با بعد متناهی روی حلقهٔ بخشی D باشد. هرگاه A و B مدولهای وفادار ساده‌ای روی حلقهٔ درونریختی $R = Hom_D(V,V)$ باشند، آنگاه A و B ، R ـ مدولهای یکریختی هستند.*

برهان. بنابر قضایای VII ۴۰۱۰، VIII ۴۰۱۰، و نتیجهٔ VIII ۱۲۰۱۰، حلقهٔ R شامل یک ایده‌آل چپ مینیمال (ناصفر) مانند I است. چون A وفادار است، $a \in A$ ای هست به‌طوری که $Ia \neq 0$. لذا، Ia یک زیرمدول ناصفر A می‌باشد (تمرین IV ۳۰۱۰)، که از آنجا، طبق سادگی، $Ia = A$. نگاشت $\theta : I \to Ia = A$ داده شده با $i \mapsto ia$ یک بروریختی R ـ مدولهاست. بنابر لم ۱۰۰۱، θ یک یکریختی است. به همین نحو، $I \cong B$.

لم ۱۶۰۱ . فرض کنیم V یک فضای‌برداری‌ناصفرروی حلقهٔ بخشی D بوده و R حلقهٔ درونریختی $Hom_D(V,V)$ باشد . هرگاه $g : V \to V$ یک همریختی گروههای جمعی باشد به طوری که به‌ازای هر $r \in R$ ، $gr = rg$ ، آنگاه $d \in D$ ای وجود دارد به قسمی که به‌ازای هر $v \in V$ ، $g(v) = dv$.

برهان . فرض کنیم u عنصر ناصفری از V باشد . حکم می‌کنیم که u و $g(u)$ روی D وابستهٔ خطی‌اند . اگر $\dim_D V = 1$ ، این بدیهی است . فرض کنیم $\dim_D V \geq 2$ و $\{u, g(u)\}$ مستقل‌خطی باشد . چون R در خودش چگال است (مثال بعد از تعریف ۸۰۱) ، $r \in R$ ی وجود دارد به‌طوری که $r(u) = 0$ و $r(g(u)) \neq 0$. اما ، طبق فرض ،

$$r(g(u)) = rg(u) = gr(u) = g(r(u)) = g(0) = 0,$$

که یک تناقض است . بنابراین ، به‌ازای $d \in D$ ای ، $g(u) = du$. هرگاه $v \in V$ ، آنگاه ، بنابر چگال بودن ، $s \in R$ ی وجود دارد به‌طوری که $s(u) = v$. درنتیجه ، چون $s \in R = \mathrm{Hom}_D(V,V)$ ، $g(v) = g(s(u)) = gs(u) = sg(u) = s(du) = ds(u) = dv$.

حکم ۱۷۰۱ . به‌ازای $i = 1,2$ ، فرض کنیم V_i یک فضای‌برداری با بعد متناهی n_i روی حلقهٔ بخشی D_i باشد .

(یک) هرگاه یک یکریختی حلقه‌ها مانند $Hom_{D_1}(V_1,V_1) \cong Hom_{D_2}(V_2,V_2)$ موجود باشد ، آنگاه $dim_{D_1}V_1 = dim_{D_2}V_2$ و D_1 با D_2 یکریخت است .

(دو) هرگاه یک‌یکریختی حلقه‌ها مانند $Mat_{n_1}D_1 \cong Mat_{n_2}D_2$ موجود باشد ، آنگاه $n_1 = n_2$ و D_1 با D_2 یکریخت است .

طرح برهان . (یک) به‌ازای $i = 1,2$ ، مثال بعد از تعریف ۵۰۱ نشان می‌دهد که V_i یک $\mathrm{Hom}_{D_i}(V_i,V_i)$ ــ مدول سادهٔ وفادار است . فرض کنیم $R = \mathrm{Hom}_{D_1}(V_1,V_1)$ و

$$\sigma : R \to \mathrm{Hom}_{D_2}(V_2,V_2)$$

یک یکریختی باشد . در این صورت ، با برگرداندن در امتداد σ ، V_2 یک R ــ مدول سادهٔ وفادار است (یعنی ، به‌ازای $r \in R, v \in V_2$ ، $rv = \sigma(r)v$) . بنابرلم ۱۵۰۱ ، یک یکریختی R ــ مدولها مانند $\phi : V_1 \to V_2$ وجود دارد . به‌ازای هر $v \in V_1$ و $f \in R$ ،

$$\phi[f(v)] = f\phi(v) = (\sigma f)[\phi(v)],$$

که از آنجا ، به عنوان یک همریختی گروههای جمعی $V_2 \to V_2$ ،

$$\phi f \phi^{-1} = \sigma(f).$$

بـه‌ازای هـر $d \in D_1$ ، فـرض کنیـم $\alpha_d : V_1 \to V_1$ همریختی گروههای جمعی باشد که با $x \mapsto dx$ تعـریف مـی‌شود . واضـح اسـت که $d = 0$ اگر و فقط اگر $\alpha_d = 0$. به‌ازای هر $f \in R = \mathrm{Hom}_{D_1}(V_1, V_1)$ و هر $d \in D_1$ ، $f\alpha_d = \alpha_d f$. درنتیجه ،

$$[\phi\alpha_d\phi^{-1}](\sigma f) = \phi\alpha_d\phi^{-1}\phi f\phi^{-1} = \phi\alpha_d f\phi^{-1} = \phi f\alpha_d\phi^{-1}$$
$$= \phi f\phi^{-1}\phi\alpha_d\phi^{-1} = (\sigma f)[\phi\alpha_d\phi^{-1}].$$

چون σ سورژکتیو اسـت ، لـم ۱۶.۱ (به‌ازای $V = V_2, g = \phi\alpha_d\phi^{-1}$) ایجاب می‌کند که $d^* \in D_2$ ی وجود دارد به‌طوری که $\phi\alpha_d\phi^{-1} = \alpha_{d^*}$. فرض کنیم $\tau : D_1 \to D_2$ نگاشت داده شده با $\tau(d) = d^*$ باشد . پس به‌ازای هر $d \in D_1$ ،

$$\phi\alpha_d\phi^{-1} = \alpha_{\tau(d)}.$$

تحقیق کنیدکه τ یک‌تکریختی‌حلقه‌هاست . با عکس‌کردن نقشهای D_1 و D_2 در استدلال قبل (و تعویض ϕ, σ با ϕ^{-1}, σ^{-1}) معلـوم می‌شود که به‌ازای هر $k \in D_2$ ، عنصری مانند $d \in D$ وجود دارد به‌طوری که

$$\phi^{-1}\alpha_k\phi = \alpha_d : V_1 \to V_1,$$

که از آنجا $\alpha_k = \phi\alpha_d\phi^{-1} = \alpha_{\tau(d)}$. درنتیجه ، $k = \tau(d)$ ؛ودرنتیجه ، τ سورژکتیو است . بنابراین ، τ یک یکریختی می‌باشد . به علاوه ، به‌ازای هر $d \in D_1$ و $v \in V_1$ ،

$$\phi(dv) = \phi\alpha_d(v) = \alpha_{\tau(d)}\phi(v) = \tau(d)\phi(v).$$

با استفاده از ایـن نشان دهید که $\{u_1, \ldots, u_k\}$ در V_1 ، D_1 ــ مستقل خطی است اگر و فقـط اگـر $\{\phi(u_1), \ldots, \phi(u_k)\}$ ، D_2 ــ مستقل خطـی در V_2 باشد . پس نتیجه می‌شود که $\dim_{D_1} V_1 = \dim_{D_2} V_2$.

(دو) از قسمت (یک) ، تمرین III ۱۷.۱۰ (ث) ، و قضیهٔ VII ۴.۱۰ استفاده کنید .

تمرینات

۱ . فرض کنید F میدانی با مشخص 0 بوده و $R = F[x,y]$ گروه جمعی چندجمله‌ایها از دو مجهول باشد . ضرب در R را با درنظر گرفتن پخشپذیری چنین تعریف می‌کنیم : به‌ازای هر $a \in F$ ، $ax = xa$, $ay = ya$ ، حاصلضرب x و y (با همین ترتیب) چندجمله‌ای xy طبق معمول است ، ولی حاصلضرب y و x چندجمله‌ای $xy + 1$

می‌باشد.

(آ) R حلقه است.

(ب) $yx^k = x^k y + kx^{k-1}$ و $y^k x = xy^k + ky^{k-1}$.

(پ) R ساده است. (**راهنمایی.** فرض کنید f عنصر ناصفری در ایده‌آل I از R باشد؛ در این صورت، f جمله‌ای شامل y ندارد یا $g = xf - fx$ عنصر ناصفری از I است که درجه‌اش نسبت به y از درجهٔ f نسبت به y پایین‌تر است. در حالت دوم، $xg - gx$ را درنظر بگیرید. مآلا"، یک عنصر ناصفر مانند $h \in I$ بیابید که فارغ از y باشد. اگر h غیرثابت باشد، $hy - yh$ را درنظر بگیرید. در چند مرحله، عنصر ثابت ناصفری از I به دست آورید؛ درنتیجه، $I = R$.)

(ت) R مقسوم‌علیه صفر ندارد.

(ث) R حلقهٔ بخشی نیست.

۲. (آ) هرگاه A یک R ــ مدول باشد، آنگاه A یک $R/\mathfrak{A}(A)$ ــ مدول با خاصیت $(a \in A)(r + \mathfrak{A}(A))a = ra$ نیز هست.

(ب) هرگاه A یک R ــ مدول‌چپ‌ساده‌باشد، آنگاه $R/\mathfrak{A}(A)$ یک حلقهٔ اولیه‌است.

۳. فرض کنید V یک فضای‌برداری با بعد نامتناهی روی حلقهٔ بخشی D باشد.

(آ) هرگاه F مجموعهٔ تمام $\theta \in \mathrm{Hom}_D(V,V)$ هایی باشد به‌طوری که $\mathrm{Im}\,\theta$ با بعد متناهی است، آنگاه F یک ایده‌آل حقیقی از $\mathrm{Hom}_D(V,V)$ می‌باشد. بنابراین، $\mathrm{Hom}_D(V,V)$ ساده نخواهد بود.

(ب) F خود یک حلقهٔ ساده است.

(پ) F مشمول هر ایده‌آل ناصفر $\mathrm{Hom}_D(V,V)$ می‌باشد.

(ت) $\mathrm{Hom}_D(V,V)$ آرتینی (چپ) نیست.

۴. فرض کنید V یک فضای برداری روی حلقهٔ بخشی D باشد. گوییم زیرحلقهٔ R از $\mathrm{Hom}_D(V,V)$ **متعدی n گونا** است اگر به‌ازای هر k $(1 \leq k \leq n)$ و هر زیرمجموعهٔ مستقل خطی $\{u_1, \ldots, u_k\}$ از V و هر زیرمجموعهٔ دلخواه $\{v_1, \ldots, v_k\}$ از V، $\theta \in R$ ای وجود داشته باشد به‌طوری که، به‌ازای $i = 1,2,\ldots,k$، $\theta(u_i) = v_i$.

(آ) هرگاه R متعدی یک‌گونا باشد، آنگاه R اولیه است. [**راهنمایی.** مثال بعد از تعریف ۵.۱ را امتحان کنید.]

(ب) هرگاه R متعدی دو گونا باشد، آنگاه R در $\mathrm{Hom}_D(V,V)$ چگال است.

[**راهنماییها:** با استفاده از (آ) نشان دهید که R زیرحلقهٔ چگالی از $\mathrm{Hom}_\Delta(V,V)$ است، که در آن $\Delta = \mathrm{Hom}_R(V,V)$. با استفاده از تعدی دوگونا، نشان دهید $\Delta = \{\beta_d \mid d \in D\}$، که در آن $\beta_d : V \to V$ با $x \mapsto dx$ داده می‌شود. درنتیجه، $\mathrm{Hom}_\Delta(V,V) = \mathrm{Hom}_D(V,V)$.]

۵ . هرگاه R یک حلقهٔ اولیه باشد به طوری که به ازای هر $a,b \in R$، $a(ab-ba) = (ab-ba)a$ آنگاه R یک حلقهٔ بخشی است. [**راهنمایی.** نشان دهید R با یک حلقهٔ چگال از درونریختیهای فضای برداری V روی حلقهٔ بخشی D که $\dim_D V = 1$ یکریخت می‌باشد؛ درنتیجه، $R \cong D$.]

۶ . هرگاه حلقهٔ یکدار R اولیه بوده و $e \in R$ چنان باشد که $e^2 = e \neq 0$، آنگاه
(آ) eRe زیرحلقه‌ای از R با واحد e است؛
(ب) eRe اولیه است. [**راهنمایی.** هرگاه R با حلقهٔ چگالی از درونریختیهای فضای برداری V روی حلقهٔ بخشی D یکریخت باشد، آنگاه Ve یک D ــ فضای برداری بوده و eRe با حلقهٔ چگالی از درونریختیهای Ve یکریخت است.]

۷ . هرگاه R یک حلقهٔ چگال از درونریختیهای فضای برداری V بوده و K ایده‌آل ناصفری از R باشد، آنگاه K نیز حلقهٔ چگالی از درونریختیهای V می‌باشد.

۲ رادیکال ژاکوبسون

رادیکال ژاکوبسون تعریف شد (قضیهٔ ۳۰۲) و خواص اساسی آن ارائه گردید (قضایای ۱۲۰۲ تا ۱۶۰۲). روابط بین حلقه‌های ساده، اولیه، و نیمه ساده بررسی شده (قضیهٔ ۱۰۰۲) و مثالهای متعددی عرضه گردید.

پیش از ادامهٔ بررسی ساختار حلقه‌ها، تکنیک کلیی که به کار خواهیم برد را خلاصه می‌کنیم. درحال حاضر امید چندانی به رده‌بندی تمام حلقه‌ها با تقریب یکریختی وجود ندارد. درنتیجه، سعی می‌کنیم رده‌هایی از حلقه‌ها را کشف کنیم که بتوان برای آنها قضایای ساختاری مناسبی به‌دست آورد. روش کلاسیکی برای تعیین یک چنین رده به‌قرار زیر است. یک خاصیت "بد" یا "نامطلوب" حلقه‌ها را اختیار و آن حلقه‌هایی را مطالعه می‌کنیم که این خاصیت را ندارند. برای آنکه این روش عملا" کار کند، باید چند فرض اضافی را بپذیریم.

فرض کنیم P خاصیتی از حلقه‌ها بوده و ایده‌آل [حلقهٔ] I را یک P ــ ایده‌آل

[P ـ حلقه] نامیم اگر I واجد خاصیت P باشد. فرض کنیم
(یک) نقش همریخت هر P ـ حلقه یک P ـ حلقه باشد؛
(دو) هر حلقهٔ R (یا دست‌کم هر حلقه در ردهٔ مشخصی مانند $\mathfrak{C}$) شامل یک P ـ ایده‌آل $P(R)$ (به‌نام P ـ *رادیکال* R) باشد که حاوی تمام P ـ ایده‌آلهای دیگر R است؛
(سه) P ـ رادیکال حلقهٔ خارج‌قسمتی $R/P(R)$ صفر باشد؛
(چهار) Pـرادیکال حلقهٔ $P(R)$ مساوی $P(R)$ باشد.

خاصیت P که در مفروضات (یک) تا (چهار) صدق کند یک *خاصیت رادیکال* نام دارد.

P ـ رادیکال را می‌توان سنجش درجه‌ای گرفت که یک حلقه واجد خاصیت "نامطلوب" P است. هرگاه خاصیت رادیکال P را اختیار کنیم، آنگاه می‌توان قضایای ساختاری را برای حلقه‌های "مطلوبی" یافت که P ـ رادیکال آنها صفر است. یک چنین حلقه P ـ رادیکال آزاد یا P ـ نیمه ساده نام دارد. در عمل معمولا" به خود P ـ رادیکال توجه داریم تا خاصیت P که از آن ناشی می‌شود. بنابر شرط (سه)، هر حلقهٔ واجد P ـ رادیکال دارای یک حلقهٔ خارج‌قسمتی Pـ نیمه ساده است. لذا، در بررسی حلقه‌های P ـ نیمه‌ساده، هر قدر P ـ رادیکال بزرگتر باشد، عوامل بیشتری طرد می‌شوند. مسئلهٔ اصلی یافتن رادیکالهایی است که بتوان با حذف حداقل عوامل قضایای ساختاری عمیقی به دست آورد.

ودربورن ابتدا در مطالعهٔ جبرهای با بعد متناهی رادیکال را معرفی کرد. نتایج وی بعدا" به حلقه‌های آرتینی (چپ) تعمیم یافتند. با اینحال، رادیکال ودربورن (یعنی، ایده‌آل پوچ‌توان ماکزیمال) و قضایای بسیار قوی حاصل از آن فقط در مورد حلقه‌های آرتینی (چپ) به کار می‌روند. در سالهای بعد رادیکالهای بسیار دیگری معرفی شدند. به بیان کلی، هر یک از اینها با رادیکال ودربورن در حالت آرتینی چپ یکی است، ولی برای حلقه‌های غیرآرتینی نیز تعریف شده‌اند.

هدف اصلی این بخش بررسی یکی از این رادیکالها، یعنی رادیکال ژاکوبسون است. رادیکال دیگر، یعنی رادیکال اول، در بخش ۴ مطرح می‌شود؛ همچنین، ر.ک. تمرین ۱۱.۴. برای بحث مشروحتری از رادیکالها، ر.ک. ان. ج. دیوینسکی [۲۲] یا ام.

---

1. N. J. Divinsky

گری[1] [۲۳] . قضایای جالب ناشی از آن بررسی مشروح رادیکال ژاکوبسون را توجیه می‌کنند . درواقع ، بخش ۱ با توجه به رادیکال ژاکوبسون طرح شده بود . حلقه‌هایی که نیمه ساده‌ٔ ژاکوبسون‌هستند (یعنی ، رادیکال ژاکوبسون صفر دارند) را می‌توان برحسب حلقه‌های ساده و اولیه توصیف کرد (بخش ۳) .

پیش از تعریف رادیکال ژاکوبسون به مقدماتی نیاز داریم .

تعریف ۱.۲ . گوییم ایده‌آل P از حلقه‌ٔ R ***اولیه‌ٔ چپ*** [***راست***] است اگر حلقه‌ٔ خارج‌قسمتی R/P یک حلقه‌ٔ اولیه‌ٔ چپ [راست] باشد .

تبصره . چون حلقه‌ٔ صفر مدول‌ساده‌نداردو لذا اولیه‌نیست ، R خود یک ایده‌آل اولیه‌ٔ چپ (یا راست) نخواهد بود .

تعریف ۲.۲ . گوییم عنصر a در حلقه‌ٔ R ***منتظم نمای چپ*** است اگر $r \in R$ ی باشد به‌طوری که $r + a + ra = 0$. عنصر r را یک ***معکوس‌نمای چپ*** a می‌نامند . گوییم ایده‌آل I (راست ،چپ ، یادوطرفه)از R ***منتظم نمای چپ*** است‌اگر هر عنصر I منتظم نمای‌چپ باشد . به همین نحو ، گوییم $a \in R$ ***منتظم نمای راست*** است اگر $r \in R$ ی باشد به‌طوری که $a + r + ar = 0$. معکوس‌نماهای‌راست‌وایده‌آلهای منتظم نمای راست به نحو مشابه تعریف می‌شوند .

چند تبصره . گاهی شایسته است به جای $r + a + ra$ بنویسیم $r \circ a$. هرگاه R یکدار باشد ، آنگاه a منتظم نمای چپ [راست] است اگر و فقط اگر $1_R + a$ معکوسپذیر چپ [راست] باشد (تمرین ۱) .

برای ساده شدن صورت چند نتیجه ، قرارداد زیر را (که درواقع قضیه‌ای از نظریه‌ٔ اصل موضوعی مجموعه‌هاست) می‌پذیریم .

هرگاه رده‌ٔ $\mathcal{C}$ از زیرمجموعه‌های‌حلقه‌ٔ R که‌درخاصیت داده شده‌ای صدق می‌کنند

---

1. M. Gray

تهی باشد، آنگاه $\bigcap_{I \in \mathfrak{C}} I$ مساوی R تعریف می‌شود.

قضیهٔ ۳.۲. *هرگاه R حلقه‌باشد، آنگاه ایده‌آلی مانند J(R) از R وجود دارد به‌طوری که*

(یک) J(R) اشتراک تمام صفرسازهای چپ R ــ مدولهای چپ ساده است؛

(دو) J(R) اشتراک تمام ایده‌آلهای چپ ماکزیمال منتظم R است؛

(سه) J(R) اشتراک تمام ایده‌آلهای اولیهٔ چپ R است؛

(چهار) J(R) یک ایده‌آل چپ منتظم نمای چپ است که شامل هر ایده‌آل چپ منتظم نمای چپ R می‌باشد؛

(پنج) احکام (یک) تا (چهار) در صورت تعویض "چپ" با "راست" نیز برقرارند.

قضیهٔ ۳.۲ ذیلا "ثابت شده است (ص ۶۷۱). ایده‌آل $J(R)$ **رادیکال ژاکوبسون** حلقهٔ R نام دارد. این رادیکال ابتدا برحسب منتظم نما تعریف شده بود (قضیهٔ ۳.۲ (چهار))، که یک خاصیت رادیکال به صورت تعریف شده در تبصره‌های معرفی شده در فوق است (ر.ک. ص ۶۷۷). به‌محض اینکه اهمیت نقش مدولها در بررسی حلقه‌ها روشنتر شد، توصیفهای دیگری از $J(R)$ به دست آمدند (قضیهٔ ۳.۲ (یک) تا (سه)).

چند تبصره. بنابر قضیهٔ ۳.۲ (یک) و قرارداد فوق، اگر R، R ــ مدول چپ ساده (و درنتیجه، صفرساز) نداشته باشد، $J(R) = R$. هرگاه R یکدار باشد، آنگاه هر ایده‌آل منتظم بوده و ایده‌آلهای چپ ماکزیمال همواره وجود دارند (قضیهٔ III ۱۸.۲۰)، که از آنجا، طبق قضیهٔ ۳.۲ (دو)، $J(R) \neq R$. قضیهٔ ۳.۲ (چهار) ایجاب **نمی‌کند** که $J(R)$ شامل هر عنصر منتظم نمای چپ R باشد؛ ر.ک. تمرین ۴.

برهان قضیهٔ ۳.۲ (که از ص ۶۷۱ شروع می‌شود) نیاز به پنج لم مقدماتی دارد. لمها برای ایده‌آلهای چپ بیان و اثبات می‌شوند. با اینحال، *هر یک از لمهای ۴.۲ تا ۸.۲ درصورت تعویض همه جایی "چپ" با "راست" نیز معتبر است.*

لم ۴.۲. *هرگاه $I (\neq R)$ یک ایده‌آل چپ منتظم از حلقهٔ R باشد، آنگاه I مشمول*

ایده‌آل چپ ماکزیمالی است که منتظم می‌باشد.

طرح برهان. چون I منتظم است، عنصری مانند $e \in R$ وجود دارد به‌طوری که به‌ازای هر $r \in R$ ، $r - re \in I$. لذا، هر ایده‌آل چپ J شامل I منتظم نیز هست (با همان عنصر $e \in R$). هرگاه $I \subset J$ و $e \in J$ ، آنگاه، به‌ازای هر $r \in R$ ، $r - re \in I \subset J$ ایجاب می‌کند که $r \in J$ ، که از آنجا $R = J$. با استفاده از این، تحقیق کنید که لم زرن را می‌توان درمورد مجموعهٔ $\mathcal{S}$ مرکب از تمام ایده‌آلهای چپ L با خاصیت $I \subset L \subsetneq R$ که توسط شمول جزئی مرتب شده به کار برد. هر عنصر ماکزیمال $\mathcal{S}$ یک ایده‌آل چپ ماکزیمال منتظم شامل I است.

لم ۵۰۲. *فرض کنیم R یک حلقه بوده و K اشتراک تمام ایده‌آلهای چپ ماکزیمال منتظم R باشد. در این صورت، K یک ایده‌آل چپ منتظم نمای چپ از R است.*

برهان. K بوضوح یک ایده‌آل چپ است. اگر $a \in K$، قرار می‌دهیم $T = \{r + ra \mid r \in R\}$ هرگاه $T = R$ ، آنگاه $r \in R$ ی وجود دارد به‌طوری که $r + ra = -a$. درنتیجه، $r + a + ra = 0$ ؛ و لذا، a منتظم نمای چپ است. پس کافی است نشان دهیم که $T = R$.

تحقیق کنید که T یک ایده‌آل چپ منتظم R (با $e = -a$) است. هرگاه $T \neq R$ ، آنگاه، بنابر لم ۴۰۲ ، T مشمول یک ایده‌آل چپ ماکزیمال منتظم مانند I_0 است (لذا، اگر R ایده‌آل چپ ماکزیمال منتظم نداشته باشد، $T \neq R$.) چون $a \in K \subset I_0$ ، به‌ازای هر $r \in R$ داریم $ra \in I_0$. لذا، چون $r + ra \in T \subset I_0$، باید به‌ازای هر $r \in R$ ، $r \in I_0$. درنتیجه، $R = I_0$ ، که ماکزیمالی I_0 را نقض می‌کند. بنابراین، $T = R$.

لم ۶۰۲. *فرض کنیم حلقهٔ R دارای R ــ مدول چپ ساده باشد. هرگاه I یک ایده‌آل چپ منتظم نمای چپ R باشد، آنگاه I مشمول اشتراک تمام صفرسازهای چپ R-مدولهای چپ است.*

برهان. هرگاه $I \not\subset \bigcap \mathfrak{a}(A)$ ، که در آن اشتراک روی تمام R ــ مدولهای چپ سادهٔ A

گرفته شده، آنگاه، به‌ازای R ــ مدول چپ ساده‌ای چون B ، $IB \neq 0$ ، که از آنجا، به‌ازای $b \in B$ ای ناصفر، $Ib \neq 0$. چون I یک ایده‌آل چپ است، Ib زیرمدول ناصفری از B می‌باشد. درنتیجه، بنابرسادگی، $B = Ib$ ؛ و لذا، به‌ازای $a \in I$ ای، $ab = -b$ ، چون I منتظم نمای چپ است، $r \in R$ ی وجود دارد به‌طوری که $r + a + ra = 0$. بنابراین، $-b = rb + ab + rab = (r + a + ra)b = 0b = 0$. چون این نتیجه $b \neq 0$ را نقض می‌کند، باید داشته باشیم $I \subset \cap \mathfrak{a}(A)$.

لم ۸۰۲ . *ایده‌آل P از حلقهٔ R اولیهٔ چپ است اگر و فقط اگر P صفرساز چپ یک R ــ مدول چپ ساده باشد.*

برهان. اگر P یک ایده‌آل اولیهٔ چپ باشد، A را یک R/P ــ مدول وفادار ساده می‌گیریم. تحقیق کنید که A یک R ــ مدول است، که در آن ra $(r \in R, a \in A)$ با $(r + P)a$ تعریف می‌شود. در این صورت، $RA = (R/P)A \neq 0$ و هر R ــ زیرمدول A یک R/P ــ زیرمدول A است، که از آنجا A یک R ــ مدول ساده می‌باشد. هرگاه $r \in R$ ، آنگاه $rA = 0$ اگر و فقط اگر $(r + P)A = 0$. اما $(r + P)A = 0$ اگر و فقط اگر $r \in P$ ، زیرا A یک R/P ــ مدول وفادار است. بنابراین، P صفرساز چپ R ــ مدول سادهٔ A می‌باشد.

به عکس، فرض کنیم P صفرساز چپ R ــ مدول سادهٔ B باشد. تحقیق کنید که B یک R/P ــ مدول ساده است، که در آن به‌ازای $r \in R, b \in B$ ، $(r + P)b = rb$. به علاوه، هرگاه $(r + P)B = 0$ ، آنگاه $rB = 0$ ، که از آنجا $r \in \mathfrak{a}(B) = P$ و، در R/P ، $r + P = 0$. درنتیجه، B یک R/P ــ مدول وفادار می‌باشد. بنابراین، R/P یک حلقهٔ اولیهٔ چپ است، که از آنجا P یک ایده‌آل اولیهٔ چپ R می‌باشد.

لم ۸۰۲ . *فرض کنیم I ایده‌آل چپ حلقهٔ R باشد. هرگاه I منتظم نمای چپ باشد، آنگاه I منتظم نمای راست می‌باشد.*

برهان. هرگاه I منتظم نمای چپ بوده و $a \in I$ ، آنگاه $r \in R$ ی وجود دارد به‌طوری که $r \circ a = r + a + ra = 0$. چون $r = -a - ra \in I$ ، $s \in R$ ی وجود دارد به‌طوری‌که

$s \circ r = s + r + sr = 0$ ، که از آنجا s منتظم نمای راست می‌باشد. به‌آسانی معلوم می‌شود که عمل $\circ$ شرکتپذیر است. درنتیجه،

$$a = 0 \circ a = (s \circ r) \circ a = s \circ (r \circ a) = s \circ 0 = s.$$

بنابر این، a ، و درنتیجه I ، منتظم نمای راست می‌باشد.

برهان قضیهٔ ۳۰۲. فرض کنیم $J(R)$ اشتراک تمام صفرسازهای **چپ** R ــ مدولهای **چپ** ساده باشد. هرگاه R دارای R ــ مدول چپ ساده نباشد، آنگاه، طبق قرارداد فوق، $J(R) = R$. بنابر قضیهٔ ۴۰۱، $J(R)$ ایده‌آل است. حال نشان می‌دهیم احکام (دو) تا (پنج) برای تمام ایده‌آلهای **چپ** درستند.

ابتدا ملاحظه می‌کنیم که خود R نمی‌تواند صفرساز یک R ــ مدول چپ سادهٔ A باشد (درغیراین‌صورت، $RA = 0$). این مطلب همراه با قضیهٔ ۳۰۱ و لم ۷۰۲ معادل بودن شرایط‌زیر را ایجاب می‌کنند:

(آ) $J(R) = R$؛

(ب) R دارای R ــ مدول چپ ساده نیست؛

(پ) R دارای ایده‌آل چپ ماکزیمال منتظم نیست؛

(ت) R ایده‌آل اولیهٔ چپ ندارد.

لذا، طبق قراردادفوق، احکام (دو)، (سه)، و (چهار) درصورتی درستند که $J(R) = R$.

(دو) فرض کنیم $J(R) \neq R$ و K اشتراک تمام ایده‌آلهای چپ ماکزیمال منتظم R باشد. بنابر لمهای ۵۰۲ و ۶۰۲، $K \subset J(R)$. به عکس، فرض کنیم $c \in J(R)$. بنابر قضیهٔ ۳۰۱، $J(R)$ اشتراک صفرسازهای چپ خارج‌قسمتهای R/I است، که در آن I تمام ایده‌آلهای چپ ماکزیمال منتظم R را می‌گیرد. به‌ازای هر ایده‌آل ماکزیمال منتظم I، $e \in R$ ای وجود دارد به‌طوری که $c - ce \in I$. چون $c \in \alpha(R/I)$، به‌ازای هر $r \in R$، $cr \in I$؛ بخصوص، $ce \in I$. درنتیجه، به‌ازای هر ایده‌آل ماکزیمال منتظم I، $c \in I$. لذا، $K = \cap I \subset J(R)$. بنابراین، $J(R) = K$.

حکم (سه) نتیجهٔ فوری لم ۷۰۲ است.

(چهار) بنابر (دو) و لم ۵۰۲، $J(R)$ یک ایده‌آل چپ منتظم نمای چپ است. بنابر لم ۶۰۲، $J(R)$ شامل هر ایده‌آل چپ منتظم نمای چپ می‌باشد.

برای اتمام برهان باید نشان داد که قسمتهای (یک) تا (چهار) پس از تعویض

"چپ" به "راست" درستند. فرض‌کنیم $J_1(R)$ اشتراک صفرسازهای *راست* تمام R ـ مدولهای *راست* ساده باشد. در این صورت، برهان قبل پس از تعویض "چپ" به "راست" معتبر است؛ درنتیجه، قسمتهای (یک) تا (چهار) برای ایده‌آل $J_1(R)$ برقرار می‌باشند. چون بنابر (چهار) ولم ۸.۲ $J(R)$ منتظم نمای راست است، بنابر (چهار)، $J(R) \subset J_1(R)$. به همین نحو، $J_1(R)$ منتظم نمای چپ می‌باشد، که از آنجا $J_1(R) \subset J(R)$. بنابراین، $J(R) = J_1(R)$.

مثال. فرض کنیم R حلقه‌ای موضعی با ایده‌آل ماکزیمال منحصر به فرد M (مرکب از تمام غیریکه‌های R؛ ر.ک. قضیهٔ III ۱۳.۴۰) باشد. نشان می‌دهیم که $J(R) = M$. چون R یکدار است، $J(R) \neq R$. چون بنابر قضیهٔ III ۲.۳۰ هر ایده‌آل حقیقی فقط شامل غیر یکه‌ها است، $J(R) \subset M$. از آن سو، هرگاه $r \in M$، آنگاه $1_R + r \notin M$ (در غیر این صورت، $1_R \in M$). درنتیجه، $1_R + r$ یکه‌است، که از آنجا r منتظم نمای چپ می‌باشد (تمرین ۱). لذا، طبق قضیهٔ ۳.۲ (چهار)، $M \subset J(R)$. بنابراین، $J(R) = M$. در اینجا دو حالت خاص وجود دارند:

مثال. بنابر نتیجهٔ III ۱۰.۵۰، حلقهٔ سری توانی $F[[x]]$ روی میدان F یک حلقهٔ موضعی با ایده‌آل ماکزیمال اصلی (x) است. بنابراین، $J(F[[x]]) = (x)$.

مثال. هرگاه p اول باشد، آنگاه Z_{p^n} $(n \geq 2)$ یک حلقهٔ موضعی با ایده‌آل ماکزیمال اصلی (p) است، که *به عنوان یک گروه آبلی* با $Z_{p^{n-1}}$ یکریخت است. بنابراین، $J(Z_{p^n}) = (p)$. رادیکال Z_m (m دلخواه) در تمرین ۱۰ درنظر گرفته شد.

تعریف ۹.۲. گوییم حلقهٔ R **نیمه ساده** (ژاکوبسون) است اگر رادیکال ژاکوبسون آن J(R) صفر باشد. گوییم R یک *حلقهٔ رادیکال* است اگر J(R) = R.

تبصره. در سراسر این کتاب "رادیکال" همواره به معنی "رادیکال ژاکوبسون" و "نیمه ساده" به معنی "نیمه سادهٔ ژاکوبسون" است. در یک قضیهٔ خاص در مطالعهٔ نظریهٔ حلقه‌ها باید مشخص شود که چه مفهومی از رادیکال و نیمه ساده به کار رفته است. درچند

تعریف از رادیکال (و نیمه سادگی) لازم است حلقه آرتینی (چپ) باشد. این در مورد رادیکال ژاکوبسون، که برای هر حلقه تعریف شده است، چنین نیست.

مثال. بنابر قضیهٔ ۳.۲ (دو)، هـر حلقهٔ بخشی نیمه ساده است، زیرا تنها ایده‌آل چپ ماکزیمال منتظم ایده‌آل صفر می‌باشد.

مثال. بنابر قضیهٔ III ۴.۳۰، هر ایده‌آل ماکزیمال در $\mathbf{Z}$ به شکل (p) است که در آن p اول می‌بـاشد. درنتیجـه، $J(\mathbf{Z}) = \bigcap_p (p) = 0$، که از آنجا $\mathbf{Z}$ نیمه‌سادهٔ ژاکوبسون می‌باشد. برای تعمیم، ر.ک. تمرین ۹.

مثال. هرگاه D حلقهٔ بخشی باشد، آنگاه حلقهٔ چندجمله‌ای

$$R = D[x_1, x_2, \ldots, x_m]$$

نیمه‌ساده‌است. زیرا هرگاه $f \in J(R)$، آنگاه، بنابر قضیهٔ ۳.۲ (چهار)، f منتظم‌نمای راست و چـپ می‌باشد. درنتیجه، بنابر تمرین ۱، $1_R + f = 1_D + f$ یکه خواهد بود. چون تنها یکه‌ها در R عناصر ناصفر D اند (ر.ک. قضیهٔ III ۱.۶۰)، نتیجه می‌شود که $f \in D$. لذا، $J(R)$ یک ایـده‌آل D است، که‌ازآنجا بنابر سادگی D، $J(R) = 0$ یا $J(R) = D$. چون $-1_D \notin J(R)$، منتظـم نمـای چـپ نیست (تحقیق کنید!). بنابراین، $J(R) = 0$ و R نیمه ساده می‌باشد.

قضیهٔ ۱۰.۲. *فرض کنیم R یک حلقه باشد.*

(یک) هرگاه R اولیه باشد، آنگاه R نیمه ساده می‌باشد.

(دو) هرگاه R ساده و نیمه ساده باشد، آنگاه R اولیه است.

(سه) هرگاه R ساده بـاشد، آنـگاه R یا یک حلقهٔ نیمه سادهٔ اولیه است یا رادیکال می‌باشد.

برهان. (یک) R دارای یک R ــ مدول چپ سادهٔ وفادار مانند A است، که از آنجا $J(R) \subset \alpha(A) = 0$. (دو) بنابرسادگی، $R \neq 0$. بایدیک R ــ مدول چپ ساده مانند A موجود بـاشد. (درغیر این صورت، طبق قضیهٔ ۳.۲ (یک)، $J(R) = R \neq 0$، که

نیمه سادگی را نقض می‌کند) . بنابر قضیهٔ ۴۰۱ صفرساز چپ $\alpha(A)$ ایده‌آلی از R است و $\alpha(A) \neq R$ (زیرا $RA \neq 0$) . درنتیجه ،طبق‌سادگی ، $\alpha(A) = 0$ ، که از آنجا A یک R ــ مدول وفادار ساده می‌باشد . بنابراین ، R اولیه خواهد بود .
(سه) هرگاه R ساده باشد ، آنگاه ایده‌آل $J(R)$ یا R است یا صفر . در حالت اول ، R یک حلقهٔ رادیکال است و در حالت دوم ، بنابر (دو) ، R نیمه ساده و اولیه می‌باشد .

چند مثال . بنابر قضیهٔ ۱۰۰۲ (یک) و مثال بعد از تعریف ۵۰۱ ، حلقهٔ درونریختی یک فضای برداری (چپ) روی یک حلقهٔ بخشی نیمه ساده است . درنتیجه ، طبق قضیهٔ VII ۴۰۱۰ ، حلقهٔ تمام ماتریسهای $n \times n$ روی یک حلقهٔ بخشی نیمه ساده است .

مثال . مثالی از یک حلقهٔ‌رادیکال‌ساده در ای . ساسیادا[1] و پی . ام . کوهن[2] [۶۶] ذکر شده است .

رادیکال کلاسیک ودربورن (در یک حلقهٔ آرتینی چپ) ایده‌آل پوچ‌توان ماکزیمال است . حال رابطهٔ بین این رادیکال و رادیکال ژاکوبسون را کشف می‌کنیم .

تعریف ۱۱۰۲ . یک عنصر حلقهٔ R **پوچ‌توان** است اگر به‌ازای عدد صحیح مثبتی چون n ، $a^n = 0$. ایده‌آل (چپ ، راست ، دوطرفهٔ) I از R **پوچ** است اگر هر عنصر I پوچ توان باشد ؛ I **پوچ‌توان** است اگر به‌ازای عدد صحیحی مانند n ، $I^n = 0$.

هر ایده‌آل پوچ‌توان پوچ است ، زیرا $I^n = 0$ ایجاب می‌کند که به‌ازای هر $a \in I$ ، $a^n = 0$. اما ممکن است یک ایده‌آل پوچ داشته باشیم که پوچ‌توان نباشد (تمرین ۱۱) .

قضیهٔ ۱۲۰۲ . *هرگاه R حلقه باشد ،آنگاه هر ایده‌آل راست یا چپ پوچ مشمول رادیکال J(R) است .*

تبصره . قضیه فورا" ایجاب می‌کند که هر حلقهٔ پوچ یک حلقهٔ رادیکال باشد .

---

1. E. Sasiada 2. P.M. Cohn

برهان ۱۲۰۲ . اگر $a^n = 0$ ، قرار می‌دهیم $r = -a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}$. تحقیق کنید که $r + a + ra = 0 = a + r + ar$ ، که‌ازآنجا a منتظم‌نمای‌چپ و راست است . بنابراین ، هر ایده‌آل چپ [راست] پوچ منتظم نمای چپ [راست] است . و در نتیجه ، بنابر قضیهٔ ۳۰۲ (چهار) ، مشمول $J(R)$ می‌باشد .

حکم ۱۳۰۲ . هرگاه R یک حلقهٔ آرتینی چپ [راست] باشد ، آنگاه رادیکال J(R) یک ایده‌آل پوچ‌توان است . درنتیجه ، هر ایده‌آل چپ یا راست پوچ از R پوچ‌توان بوده و J(R) ایده‌آل چپ (یا راست) پوچ‌توان ماکزیمال منحصر به فردی از R می‌باشد .

تبصره . هرگاه R نوتری چپ [راست] باشد ، آنگاه هر ایده‌آل چپ یا راست پوچ‌توان است (تمرین ۱۶) .

برهان ۱۳۰۲ . فرض کنیم $J = J(R)$ و زنجیر $J \supset J^2 \supset J^3 \supset \cdots$ از ایده‌آلهای (چپ) را درنظرمی‌گیریم . طبق‌فرض ، k ای وجوددارد به‌طوری که به‌ازای هر $i \geq k$ ، $J^i = J^k$. حکم می‌کنیم که $J^k = 0$. هرگاه $J^k \neq 0$ ، آنگاه‌مجموعهٔ S مرکب از تمام ایده‌آلهای چپ I که $J^k I \neq 0$ ناتهی است (زیرا $J^k J^k = J^{2k} = J^k \neq 0$) . بنابر قضیهٔ VIII ۴۰۱۰ ، S دارای عنصر مینیمال I_0 است . چون $J^k I_0 \neq 0$ ، عنصر ناصفری چون $a \in I_0$ وجود دارد به‌طوری که $J^k a \neq 0$. واضح است که $J^k a$ یک ایده‌آل چپ از R است که مشمول I_0 می‌باشد . به علاوه ، $J^k a \in S$ ، زیرا $J^k(J^k a) = J^{2k}a = J^k a \neq 0$. درنتیجه ، بنابر مینیمالی ، $J^k a = I_0$. لذا ، به‌ازای‌عنصرناصفری‌چون $r \in J^k$ ، $ra = a$. چون‌داریم $-r \in J^k \subset J(R)$ ، $-r$ منتظم نمای چپ است ، که از آنجا به‌ازای $s \in R$ ی ، $s - r - sr = 0$. درنتیجه ،

$$a = ra = -[-ra] = -[-ra + 0] = -[-ra + sa - sa]$$
$$= -[-ra + sa - s(ra)] = -[-r + s - sr]a = -0a = 0.$$

این امر $a \neq 0$ را نقض می‌کند . بنابراین ، $J^k = 0$. حال آخرین حکم قضیه فورا " از قضیهٔ ۱۲۰۲ نتیجه می‌شود .

بالاخره ، می‌خواهیم نشان‌دهیم که انتظام نمای چپ یک خاصیت رادیکال به صورت تعریف‌شده‌در مقدمهٔ‌این‌بخش است . بنابر قضیهٔ ۳۰۲ (چهار) ، واضح است که رادیکال

مربوط بـه آن رادیکال ژاکـوبسون است و هر حلقهٔ منتظم نمای چپ دقیقا " یک حلقهٔ رادیکال‌است (تعریف ۹.۲) . چون یک همریختی حلقه‌ها لزوما " عناصر منتظم نمای چپ را به روی عناصر منتظـم نمای چپ می‌نگارد ، پس نقش همریخت هر حلقهٔ رادیکال نیز حلقهٔ رادیکال اسـت . برای اتمام بحث باید نشان دهیم که $R/J(R)$ نیمه ساده بوده و $J(R)$ یک حلقهٔ رادیکال می‌باشد .

قضیهٔ ۱۴.۲ . هرگاه R حلقه‌باشد ،آنگاه حلقهٔ خارج‌قسمتی R/J(R) نیمه ساده است .

برهان . فرض کنیم $\pi : R \to R/J(R)$ بروریختی‌کانونی‌بوده‌و $\pi(r)$ را با $\bar{r}$ $(r \in R)$ نشان می‌دهیم . همچنین ، $\mathcal{C}$ مجموعهٔ تمام ایده‌آلهای چپ ماکزیمال منتظم R باشد . هرگاه $I \in \mathcal{C}$ ، آنگـاه، بنابر قضیهٔ ۳.۲ (دو) ، $J(R) \subset I$ ، و، بنابر قضیهٔ IV ۱۰.۱۰ ، $\pi(I) = I/J(R)$ یک ایـده‌آل چپ ماکزیمال $R/J(R)$ می‌باشد . هرگاه $e \in R$ چنان باشد که به‌ازای هر $r \in R$ ، $r - re \in I$ ، آنگاه‌به‌ازای هر $\bar{r} \in R/J(R)$ ، $\bar{r} - \bar{r}\bar{e} \in \pi(I)$. بنابراین ، به‌ازای هر I در $\mathcal{C}$ ، $\pi(I)$ منتظم است . چون $J(R) = \bigcap_{I \in \mathcal{C}} I$ ، به‌آسانی تحقیق می‌شود که هرگاه $\bar{r} \in \bigcap_{I \in \mathcal{C}} \pi(I) = \bigcap_{I \in \mathcal{C}} I/J(R)$ ، آنگاه $r \in J(R)$. درنتیجه، بنابر قضیهٔ ۳.۲ (دو) (اعمال شده بر $R/J(R)$) ،

$$J(R/J(R)) \subset \bigcap_{I \in \mathcal{C}} \pi(I) \subset \pi(J(R)) = 0,$$

که از آنجا $R/J(R)$ نیمه ساده می‌باشد .

لم ۱۵.۲ . فرض‌کنیم R حلقه بوده و $a \in R$.
(یک) هرگاه $-a^2$ منتظم نمای چپ باشد ، آنگاه a نیز چنین است .
(دو) $a \in J(R)$ اگر و فقط‌اگر Ra یک ایده‌آل چپ منتظم نمای چپ باشد.

برهان . (یک) اگر $r + (-a^2) + r(-a^2) = 0$ ، قرارمی‌دهیم $s = r - a - ra$. تحقیق کنید که $s + a + sa = 0$ ، که از آنجا a منتظم نمای چپ است .
(دو) هرگاه $a \in J(R)$ ، آنگاه $Ra \subset J(R)$. بنابراین ، Ra منتظم نمای چپ است ، زیرا

$J(R)$ چنین است. به عکس، فرض کنیم Ra منتظم نمای چپ باشد. تحقیق کنید که $K = \{ra + na \mid r \in R, n \in \mathbf{Z}\}$ یک ایده‌آل چپ R است که شامل a و Ra می‌باشد. هرگاه $s = ra + na$، آنگاه $-s^2 \in Ra$. طبق فرض، s^2 منتظم نمای چپ است؛ و درنتیجه، بنابر (یک)، s چنین است. لذا، K یک ایده‌آل چپ منتظم نمای چپ است. پس، طبق قضیهٔ ۳۰۲ (چهار)، $a \in K \subset J(R)$.

قضیهٔ ۱۶۰۲. **(یک) هرگاه ایده‌آل I حلقهٔ R خود یک حلقه ملحوظ شود، آنگاه $J(I) = I \cap J(R)$.**
(دو) هرگاه R نیمه ساده باشد، آنگاه هر ایده‌آل R نیز چنین است.
(سه) $J(R)$ یک حلقهٔ رادیکال است.

برهان. (یک) $I \cap J(R)$ بوضوح ایده‌آلی از I است. هرگاه $a \in I \cap J(R)$، آنگاه a منتظم نمای چپ در R است، که از آنجا به‌ازای $r \in R$ ی، $r + a + ra = 0$. اما $r = -a - ra \in I$. لذا، هر عنصر $I \cap J(R)$ منتظم نمای چپ در I است. بنابراین، طبق قضیهٔ ۳۰۲ (چهار) (اعمال شده بر I)، $I \cap J(R) \subset J(I)$.

فرض کنیم $a \in J(I)$. به‌ازای هر $r \in R$، $-(ra)^2 = -(rar)a \in IJ(I) \subset J(I)$؛ که از آنجا، طبق قضیهٔ ۳۰۲ (چهار)، $-(ra)^2$ منتظم نمای چپ است. درنتیجه، طبق لم ۱۵۰۲ (یک)، ra منتظم نمای‌چپ در I و لذا در R است. لذا، Ra یک ایده‌آل چپ منتظم نمای چپ R است، که از آنجا، طبق لم ۱۵۰۲ (دو)، $a \in J(R)$. بنابراین، $a \in J(I) \cap J(R) \subset I \cap J(R)$. درنتیجه، $J(I) \subset I \cap J(R)$، که برهان $J(I) = I \cap J(R)$ را تمام می‌کند. حال احکام (دو) و (سه) نتایج فوری (یک) می‌باشند.

قضیهٔ ۱۷۰۲. **هرگاه $\{R_i \mid i \in I\}$ خانواده‌ای از حلقه‌ها باشد، آنگاه $J(\prod_{i \in I} R_i) = \prod_{i \in I} J(R_i)$.**

طرح برهان. تحقیق کنید که یک عنصر $\{a_i\} \in \prod R_i$ در $\prod R_i$ منتظم نمای چپ است اگر و فقط اگر به‌ازای هر i، a_i در R_i منتظم نمای چپ باشد. درنتیجه، $\prod J(R_i)$ یک

ایده‌آل منتظم نمای چپ از $\prod R_i$ است، که از آنجا، طبق قضیهٔ ۳.۲ (چهار)، $\prod J(R_i) \subset J(\prod R_i)$.

به‌ازای هر $k \in I$، فرض می‌کنیم $\pi_k : \prod R_i \to R_k$ تصویرکانونی باشد. تحقیق کنید که $I_k = \pi_k(J(\prod R_i))$ یک ایده‌آل منتظم نمای چپ R_k است. پس نتیجه می‌شود که $I_k \subset J(R_k)$؛ و از اینرو، $J(\prod R_i) \subset \prod J(R_i)$.

تمرینات

تذکر. R همواره یک حلقه است.

۱. فرض کنید به‌ازای هر $a,b \in R$، $a \circ b = a + b + ab$.

(آ) $\circ$ یک عمل دوتایی شرکتپذیر با عنصر همانی $0 \in R$ است.

(ب) مجموعهٔ G مرکب ازتمام عناصر R که منتظم نمای چپ و راست باشد تحت $\circ$ گروه تشکیل می‌دهد.

(پ) هرگاه R یکدارباشد، آنگاه $a \in R$ منتظم نمای چپ [راست] است اگر و فقط اگر $1_R + a$ معکوسپذیر چپ [راست] باشد.

[**راهنمایی.** $(1_R + r)(1_R + a) = 1_R + r \circ a$ و $r(1_R + a) - 1_R = (r - 1_R) \circ a$]

۲. (کاپلانسکی) R حلقهٔ بخشی است اگر و فقط اگر هر عنصر R جز یکی منتظم نمای چپ باشد. [توجه کنید که تنها عنصر حلقهٔ بخشی D که منتظم نمای چپ **نیست** عبارت است از -1_D؛ همچنین، ر.ک. تمرین ۱].

۳. فرض کنید I یک ایده‌آل چپ از R بوده و $(I : R) = \{r \in R \mid rR \subset I\}$.

(آ) $(I : R)$ ایده‌آلی از R است. هرگاه I منتظم باشد، آنگاه $(I : R)$ بزرگترین ایده‌آلی از R است که مشمول I می‌باشد.

(ب) هرگاه I یک ایده‌آل چپ ماکزیمال منتظم R بوده و $A \cong R/I$، آنگاه $\alpha(A) = (I : R)$. بنابراین، $J(R) = \cap (I : R)$، که‌درآن I تمام ایده‌آلهای چپ ماکزیمال منتظم R را می‌گیرد.

۴. رادیکال $J(R)$ شامل خودتوان ناصفر نیست. اما یک خودتوان ناصفر ممکن است منتظم نمای چپ باشد [**راهنمایی.** تمرینهای ۱ و ۲].

۵ . هرگاه R یکدار باشد، آنگاه

(آ) $J(R) = \{r \in R \mid 1_R + sr$ ، $s \in R$ معکوسپذیر چپ است$\}$.

(ب) $J(R)$ بزرگترین ایده‌آل K است بـه‌طوری که به‌ازای هر $r \in K$ ، $1_R + r$ یکه است .

۶ . (آ) نقش همریخت یک حلقهٔ نیمه ساده لزوما" نیمه ساده نیست .

(ب) هرگاه $f : R \to S$ یک بروریختی حلقه‌ها باشد، آنگاه $f(J(R)) \subset J(S)$.

۷ . هرگاه R حلقهٔ تمام‌اعداد گویا با مخرج فرد باشد، آنگاه $J(R)$ از تمام اعداد گویا با مخرج فرد و صورت زوج تشکیل شده است .

۸ . فرض کنید R حلقهٔ تمام ماتریسهای $n \times n$ بالا مثلثی روی حلقهٔ بخشی D باشد (ر.ک. تمرین VII ۲۰۱۰) . $J(R)$ را یافته و ثابت کنید $R/J(R)$ با حاصلضرب مستقیم $D \times D \times \cdots \times D$ (n عامل) یکریخت است .

[**راهنمایی .** نشان دهید که یک ماتریس اکیدا" مثلثی پوچ‌توان است .]

۹ . دامنهٔ ایده‌آل‌اصلی R نیمه‌ساده‌است اگر و فقط‌اگر R یک میدان بوده یا R شامل بی‌نهایت عنصر تحویل‌ناپذیر شرکت ناپذیر متمایز باشد .

۱۰ . فرض کنید D یک دامنهٔ ایده‌آل‌اصلی بوده و d یک عنصر غیریکهٔ ناصفر D باشد . همچنین، R حلقهٔ خارج قسمتی $D/(d)$ باشد .

(آ) R نیمه ساده است اگر و فقط‌اگر d حاصلضرب عناصر تحویل‌ناپذیر شرکت ناپذیر متمایز D باشد . [**راهنمایی .** تمرین VIII ۲۰۱۰ .]

(ب) $J(R)$ چیست؟

۱۱ . اگر p اول‌باشد، R رازیرحلقهٔ $\sum_{n\geq 1} Z_{p^n}$ از $\prod_{n\geq 1} Z_{p^n}$ بگیرید . ایده‌آل $I = \sum_{n\geq 1} I_n$ ، که در آن ایده‌آل I_n از Z_{p^n} تولید شده به وسیلهٔ $p \in Z_{p^n}$ است، یک ایده‌آل پوچ R است که پوچ‌توان نیست .

۱۲ . فرض کنید حلقهٔ R یکدارنباشد . مثل قضیهٔ III ۱۰۱۰ ، R را در حلقهٔ یکدار S که مشخص صفردارد بنشانید . ثابت کنید $J(R) = J(S)$. درنتیجه، هر حلقهٔ نیمه ساده را می‌توان در یک حلقهٔ نیمه سادهٔ یکدار نشانید .

۱۳ . $J(\mathrm{Mat}_n R) = \mathrm{Mat}_n J(R)$. برهان را به اختصار ذکر می‌کنیم :

(آ) اگر A یک R ــ مدول‌چپ‌باشد، عناصر $A^n = A \oplus A \oplus \cdots \oplus A$ (n جمعوند) را بردارهایی ستونی بگیرید؛ در این صورت، A^n (تحت ضرب ماتریسی معمولی)

یک $(\mathrm{Mat}_n R)$ ــ مدول چپ است.

(ب) اگر A یک R ــ مدول ساده باشد، A^n یک $(\mathrm{Mat}_n R)$ ــ مدول ساده است.

(پ) $J(\mathrm{Mat}_n R) \subset \mathrm{Mat}_n J(R)$.

(ت) $\mathrm{Mat}_n J(R) \subset J(\mathrm{Mat}_n R)$. [**راهنمایی.** به طریق زیر ثابت کنید $\mathrm{Mat}_n J(R)$ یک ایده‌آل منتظم نمای چپ $\mathrm{Mat}_n R$ است. به‌ازای هر $k = 1, 2, \ldots, n$، فرض کنید K_k از تمام ماتریسهای (a_{ij}) تشکیل شده باشد که $a_{ij} \in J(R)$ و، اگر $j \neq k$، $a_{ij} = 0$. نشان دهید که K_k یک ایده‌آل چپ منتظم نمای چپ $\mathrm{Mat}_n R$ است و توجه کنید که $K_1 + K_2 + \cdots + K_n = \mathrm{Mat}_n J(R)$.]

۱۴. (آ) فرض کنید I یک ایده‌آل ناصفر $R[x]$ بوده و $p(x)$ یک چندجمله‌ای ناصفر از کوچکترین درجه در I باضریب‌پیشرو a باشد. هرگاه $f(x) \in R[x]$ و $a^m f(x) = 0$، آنگاه $a^{m-1} p(x) f(x) = 0$.

(ب) هرگاه حلقهٔ R ایده‌آل پوچ ناصفر نداشته باشد (بخصوص، R نیمه ساده باشد)، آنگاه $R[x]$ نیمه ساده است. [**راهنمایی.** فرض کنید M مجموعهٔ چندجمله‌ایهای ناصفر ازکوچکترین درجه در $J(R[x])$ باشد. همچنین، N مجموعهٔ مرکب از 0 و ضرایب پیشرو چندجمله‌ایها در M باشد. با استفاده از (آ)، نشان دهید N یک ایده‌آل پوچ R است، که از آنجا $J(R[x]) = 0$.]

(پ) حلقه‌هایی مانند R وجود دارندکه $R[x]$ نیمه ساده است، ولی R این‌طور نیست. [**راهنمایی.** $R = F[[x]]$ را که در آن F میدان‌است‌درنظربگیرید.]

۱۵. فرض کنید L یک ایده‌آل چپ و K یک ایده‌آل راست R باشد. همچنین، $M(R)$ ایده‌آل تولید شده به وسیلهٔ **تمام** ایده‌آلهای پوچ‌توان R باشد.

(آ) $L + LR$ ایده‌آلی است که به‌ازای هر $n \geq 1$، $(L + LR)^n \subset L^n + L^n R$.

(ب) $K + RK$ ایده‌آلی است که به‌ازای هر $n \geq 1$، $(K + RK)^n \subset K^n + RK^n$.

(پ) اگر L [یا K] پوچ‌توان باشد، ایده‌آل $L + LR$ [یا $K + RK$] نیز چنین است، که از آنجا $L \subset M(R)$ [یا $K \subset M(R)$].

(ت) هرگاه N یک ایده‌آل پوچ‌توان ماکزیمال R باشد، آنگاه R/N ایده‌آل پوچ توان ناصفر چپ یا راست ندارد. [**راهنمایی.** ابتدا نشان دهید که R/N ایده‌آل پوچ‌توان‌ناصفرندارد؛ سپس‌قسمت(پ) را در مورد حلقهٔ R/N اعمال نمایید.]

(ث) هرگاه K [یا L] پوچ بوده ولی پوچ توان نباشد و $\pi : R \to R/N$ برووریختی

کانونی باشد، آنگاه $\pi(K)$ [یا $\pi(L)$] یک ایده‌آل راست [چپ] پوچ R/N است که پوچ‌توان نیست.

۱۶. (لویتسکی[1]) هرایده‌آل چپ‌یاراست‌پوچ I درحلقهٔ نوتری چپ R پوچ‌توان است.
[*طرح برهان*. بنابر تمرین ۱۵، کافی است فرض شود R ایده‌آل پوچ‌توان ناصفر چپ یا راست ندارد. فرض کنید I ایده‌آل چپ یا راستی باشد که پوچ‌توان نیست و $a \in I$ و $a \neq 0$. نشان‌دهیدکه aR یک ایده‌آل راست‌پوچ است (حتی اگر I ایده‌آل چپ باشد)؛ درنتیجه، ایده‌آل چپ $\mathfrak{A}(u)$ به‌ازای هر $u \in aR$ ناصفر است. عنصر ناصفری مانند $u_0 \in aR$ وجود دارد که $\mathfrak{A}(u_0)$ ماکزیمال است؛ درنتیجه، به‌ازای هر $x \in R$ که $u_0x \neq 0$، $\mathfrak{A}(u_0) = \mathfrak{A}(u_0x)$. نشان دهید که به‌ازای هر $y \in R$، $(u_0y)u_0 = 0$؛ درنتیجه، $(Ru_0)^2 = 0$. بنابراین، $Ru_0 = 0$، که ایجاب می‌کند که $\{r \in R \mid Rr = 0\}$ یک ایده‌آل پوچ‌توان ناصفر راست R باشد، که تناقض است.]

۱۷. نشان دهید که لم ناکایامای VIII ۵.۴۰ برای هر حلقهٔ یکدار R معتبر است مشروط بر اینکه شرط (یک) با شرط‌زیر تعویض شود:
(یک′) J مشمول رادیکال ژاکوبسون R است.
[**راهنمایی**. با استفاده از قضیهٔ ۳.۲ (چهار) و تمرین ۱ (پ)، نشان دهیدکه (دو) $\Rightarrow$ (یک′).]

۳ حلقه‌های نیمه ساده

برای سازگاری بانظریهٔ رادیکالهاکه‌در قسمت اول بخش ۲ به اختصار ذکر شد، حلقه‌هایی را مطالعه می‌کنیم که نیمه ساده و ژاکوبسون می‌باشند. حلقه‌های نیمه سادهٔ دلخواه به عنوان انواع خاص زیر حلقه‌های حاصل‌ضربهای مستقیم حلقه‌های اولیه مشخص می‌شوند (حکم ۲.۳). نتایج بسیارقویتربرای حلقه‌های آرتینی (چپ) نیمه ساده ثابت شده‌اند. این‌حلقه‌هادرواقع حاصل‌ضربهای‌مستقیم متناهی حلقه‌های ساده می‌باشند (قضیهٔ ۳.۳). همچنین، می‌توان آنها را به طرق مختلف برحسب مدولها مشخص نمود (قضیهٔ ۷.۳). در این راه مدولهای نیمه ساده روی حلقه‌های دلخواه تعریف شده و خواص اساسی آنها عرضه خواهند شد (قضیهٔ ۶.۳).

تعریف ۱.۳. گوییم حلقهٔ R یک *حاصل‌ضرب زیر مستقیم* خانوادهٔ $\{R_i \mid i \in I\}$ از

1. Levitsky

حلقه‌هاست اگر R زیرحلقه‌ای از حاصل‌ضرب مستقیم $\prod_{i\in I} R_i$ باشد به‌طوری که به‌ازای هر $k \in I$ ، $\pi_k(R) = R_k$ ، که در آن $\pi_k : \prod_{i\in I} R_i \to R_k$ برووریختی کانونی می‌باشد .

تبصره . حلقهٔ S با یک‌حاصل‌ضرب‌زیرمستقیم‌ازخانوادهٔ $\{R_i \mid i \in I\}$ ازحلقه‌ها یکریخت است اگر و فقط‌اگر یک تکریختی از حلقه‌ها مانند $\phi : S \to \prod_{i\in I} R_i$ موجود باشد به‌طوری که به‌ازای هر $k \in I$ ، $\pi_k\phi(S) = R_k$.

مثال . فرض‌کنیم P مجموعهٔ اعداد صحیح اول باشد . به‌ازای هر $k \in \mathbf{Z}$ و $p \in P$ ، $k_p \in Z_p$ را نقش k تحت برووریختی کانونی $\mathbf{Z} \to Z_p$ می‌گیریم . در این صورت ، نگاشت $\phi : \mathbf{Z} \to \prod_{p\in P} Z_p$ داده شده با $k \mapsto \{k_p\}_{p\in P}$ یک تکریختی حلقه‌هاست به‌طوری که به‌ازای‌هر $p \in P$ ، $\pi_p\phi(\mathbf{Z}) = Z_p$. بنابراین ، $\mathbf{Z}$ باحاصل‌ضرب زیرمستقیمی از خانوادهٔ $\{Z_p \mid p \in P\}$ از میدانها یکریخت است . به‌طور کلی ، داریم :

حکم ۲۰۳ . حلقهٔ ناصفر R نیمه‌ساده‌است اگر و فقط‌اگر R با حاصل‌ضرب زیرمستقیمی از حلقه‌های اولیه یکریخت باشد .

تبصره . احکام ۷۰۱ و ۲۰۳ ایجاب می‌کنند که هر حلقهٔ نیمه سادهٔ تعویضپذیر ناصفر یک حاصل‌ضرب زیرمستقیم از میدانها باشد .

طرح برهان ۲۰۳ . فرض‌کنیم R نیمه‌ساده‌و ناصفر بوده و $\mathcal{P}$ مجموعهٔ تمام ایده‌آلهای اولیهٔ چپ R باشد . در این صورت ، به‌ازای هر $P \in \mathcal{P}$ ، R/P یک حلقهٔ اولیه است (تعریف ۱۰۲) . بنابرقضیهٔ ۳۰۲ (سه) ، $0 = J(R) = \bigcap_{P\in\mathcal{P}} P$. به‌ازای هر P ، فرض‌کنیم $\lambda_P : R \to R/P$ و $\pi_P : \prod_{Q\in\mathcal{P}} R/Q \to R/P$ برووریختیهای کانونی مربوطه باشند . نگاشت

$\phi : R \to \prod_{P \in \mathcal{P}} R/P$ داده شده با $\{r \mapsto \{\lambda_P(r)\}_{P\in\mathcal{P}} = \{r + P\}_{P\in\mathcal{P}}$ یک‌تکریختی حلقه‌هاست به‌طوری که به‌ازای هر $P \in \mathcal{P}$ ، $\pi_P\phi(R) = R/P$.

به‌عکس، فرض کنیم خانواد‌ۀ $\{R_i \mid i \in I\}$ ازحلقه‌های‌اولیه‌و تکریختی $\phi : R \to \prod_{i\in I} R_i$ از حلقه‌ها موجود باشند به‌طوری کـه به‌ازای هر $k \in I$ ، $\pi_k\phi(R) = R_k$. همچنین ، ψ_k بـرو‌ریختی $\pi_k\phi$ باشد . در ایـن صورت ، $R/\mathrm{Ker}\,\psi_k$ با حلقۀ اولیـۀ R_k یکریخت است (نتیجۀ III ۱۰.۲۰) ، که از آنجا $\mathrm{Ker}\,\psi_k$ یک ایده‌آل اولیۀ چپ R می‌باشد (تعریف ۱۰۲) . بنابراین ، طبق قضیۀ ۳۰۲ (سه) ، $J(R) \subset \bigcap_{k\in I} \mathrm{Ker}\,\psi_k$. به علاوه ، هرگاه $r \in R$ و $\psi_k(r) = 0$ ، آنگاه مولفۀ k ام $\phi(r)$ در $\prod R_i$ صفر است . لذا ، اگر $r \in \bigcap_{k\in I} \mathrm{Ker}\,\psi_k$ ، بـاید داشتـه بـاشیـم $\phi(r) = 0$. چون ϕ تکـریختـی اسـت ، $r = 0$. بنـابراین ، $J(R) \subset \bigcap_{k\in I} \mathrm{Ker}\,\psi_k = 0$ ، که از آنجا R نیمه ساده می‌باشد .

حال ، درپرتو نتایج مربوط به حلقه‌های اولیه در بخش ۱ ، می‌توان حلقه‌های نیمه ساده را حلقه‌هایی توصیف کرد که با حاصل‌ضربهای زیر مستقیم خانواده‌هایی از حلقه‌ها یکریخت است ،که‌هر یک حلقۀ چگالی‌از‌درونریختیهای یک فضای برداری روی یک حلقۀ بخشی می‌باشد . متاسفانه ،حاصل‌ضربهای زیر مستقیم (و حلقه‌های چگال از درونریختیها) همیشه مناسبترین شیٔ‌نیستند . امـا ، در صـورت عدم وجود قیود بیشتر ، این احتمالاً" بهترین کاری است‌که می‌توان انجام داد . با اینحال ، در حلقه‌های آرتینی (چپ) ،این نتایج را می‌توان به‌نحو قابل ملاحظه‌ای قوی ساخت .

قضیۀ ۳۰۳ (ودربورن ــ آرتین) . *شرایط زیر بر حلقۀ R باهم معادلند :*

(یک) *R یک حلقۀ آرتینی چپ نیمه سادۀ ناصفر است ؛*

(دو) *R حاصل‌ضرب مستقیم تعـدادی متناهی ایده‌آل ساده است که هر یک با حلقۀ*

درونریختی یک فضای برداری با بعد متناهی روی یک حلقهٔ بخشی یکریخت می‌باشد؛
(سه) *حلقه‌های بخشی* $D_1, \dots, D_t$ *و اعداد صحیح مثبت* $n_1, \dots, n_t$ *وجود دارند به طوری که* R *با حلقهٔ* $Mat_{n_1}D_1 \times Mat_{n_2}D_2 \times \cdots \times Mat_{n_t}D_t$ *یکریخت می‌باشد.*

تبصره. منظور از ایده‌آل سادهٔ R یعنی ایده‌آلی که خود یک حلقهٔ ساده می‌باشد.

برهان ۳۰۳. (سه) $\Leftrightarrow$ (دو) تمرین III ۹۰۲۰ و قضیهٔ VII ۴۰۱۰.

(یک) $\Rightarrow$ (دو) طبق فرض، $R \cong \prod_{i=1}^{t} R_i$ که در آن هر R_i حلقهٔ درونریختی یک فضای برداری است. مثال بعد از تعریف ۵۰۱ نشان می‌دهد که هر R_i اولیه است؛ طبق قضیهٔ ۱۰۰۲ (یک)، $J(R_i) = 0$. درنتیجه، طبق قضیهٔ ۱۷۰۲،

$$J(R) \cong \prod_{i=1}^{t} J(R_i) = 0.$$

بنابراین، R نیمه ساده می‌باشد. R، بنابر قضیهٔ VII ۴۰۱۰ و نتایج VIII ۷۰۱۰ و VIII ۱۲۰۱۰، آرتینی چپ است.

(دو) $\Rightarrow$ (یک) چون $R \neq 0$ و $J(R) = 0$، بنابر قضیهٔ ۳۰۲ (سه)، R دارای ایده‌آلهای اولیهٔ چپ است. فرض کنیم R فقط تعدادی متناهی ایده‌آل اولیهٔ چپ متمایز مانند $P_1, P_2, \dots, P_t$ داشته‌باشد. دراین صورت، هر R/P_i یک حلقهٔ اولیه است (تعریف ۱۰۲) که‌آرتینی چپ می‌باشد (نتیجهٔ VIII ۶۰۱۰). درنتیجه، بنابر قضیهٔ ۱۴۰۱، هر R/P_i یک حلقهٔ ساده است که با حلقهٔ درونریختی یک فضای برداری چپ با بعد متناهی روی یک‌حلقهٔ بخشی یکریخت می‌باشد. چون R/P_i ساده است، هر P_i یک ایده‌آل ماکزیمال R می‌باشد (قضیهٔ III ۱۳۰۲۰). به علاوه، $R^2 \not\subset P_i$ (در غیر این صورت، $(R/P_i)^2 = 0$)، که از آنجا، بنابر ماکزیمالی، $R^2 + P_i = R$. به همین نحو، هرگاه $i \neq j$، آنگاه، بنابر ماکزیمالی، $P_i + P_j = R$. لذا، طبق نتیجهٔ III ۲۷۰۲۰ (از قضیهٔ باقیماندهٔ چینی) و قضیهٔ ۳۰۲ (سه)، یک یکریختی حلقه‌ها مانند

$$R = R/0 = R/J(R) = R/\bigcap_{i=1}^{t} P_i \cong R/P_1 \times \cdots \times R/P_t$$

وجود دارد. هرگاه $\iota_k : R/P_k \to \prod_{i=1}^{t} R/P_i$ تکریختی کانونی باشد (قضیهٔ III ۲۲۰۲۰)،

آنگاه هر $\iota_k(R/P_k)$ یک ایده‌آل ساده از $\prod_{i=1}^{t} R/P_i$ است. نقشهای $\iota_k(R/P_k)$ تحت یکریختی $\prod_{i=1}^{t} R/P_i \cong R$ ایده‌آلهای ساده‌ای از R می‌باشند. واضح است که R حاصلضرب مستقیم (داخلی) این ایده‌آلهاست.

برای اتمام برهان کافی‌است نشان دهیم که R نمی‌تواند تعدادی نامتناهی ایده‌آل اولیهٔ چپ متمایز داشته باشد. به عکس، فرض‌کنیم $P_1, P_2, P_3, \ldots$ دنباله‌ای‌از ایده‌آلهای اولیهٔ چپ متمایز از R باشد. چون

$$P_1 \supset P_1 \cap P_2 \supset P_1 \cap P_2 \cap P_3 \supset \cdots$$

یک زنجیرکاهشی از ایده‌آلهای (چپ) است، عدد صحیحی مانند n وجود دارد به‌طوری که $P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n \cap P_{n+1}$، که ازآنجا $P_1 \cap \cdots \cap P_n \subset P_{n+1}$. بند قبل نشان می‌دهد که $R^2 + P_i = R$ و به‌ازای $i,j = 1,2,\ldots,n+1$ $(i \neq j)$، $P_i + P_j = R$. برهان‌قضیهٔ III ۲۵.۲۰ نشان‌می‌دهدکه $P_{n+1} + (P_1 \cap \cdots \cap P_n) = R$. درنتیجه، $P_{n+1} = R$، که اولیهٔ چپ بودن P_{n+1} را نقض می‌کند (ر.ک. تبصرهٔ بعد از تعریف ۱۰۲). بنابراین، R فقط تعدادی متناهی ایده‌آل اولیهٔ متمایز دارد و برهان تمام می‌باشد.

نتیجهٔ ۴۰۳. *(یک) حلقهٔ آرتینی چپ نیمه ساده یکدار است.*
(دو) یک حلقهٔ نیمه ساده آرتینی چپ است اگر و فقط اگر آرتینی راست باشد.
(سه) یک حلقهٔ آرتینی چپ نیمه ساده هم نوتری چپ است هم نوتری راست.

تبصره. درواقع، مطلب قویتری برقرار است: هر حلقهٔ آرتینی چپ یکدار نوتری چپ است (تمرین ۱۳).

طرح برهان ۴۰۳. (یک) قضیهٔ ۳۰۳. (دو) قضیهٔ ۳۰۳ درصورت تعویض "چپ" با "راست" در سراسر آن برقرار است. درنتیجه، معادل بودن شرایط (یک) و (سه) قضیهٔ ۳۰۳ ایجاب می‌کند که R آرتینی چپ است اگر و فقط اگر R آرتینی راست باشد.
(سه) نتایج VIII ۷۰۱۰ و VIII ۱۲۰۱۰ و قضیهٔ ۳۰۳ (سه).

نتیجهٔ زیر در آینده به کار نمی‌آید. به یاد آورید که عنصر e از حلقهٔ R را خودتوان گویند اگر $e^2 = e$.

نتیجهٔ ۵.۳. *هرگاه I ایده‌آلی در حلقهٔ آرتینی چپ نیمه سادهٔ R باشد، آنگاه $I = Re$، که در آن e خودتوانی است که در مرکز R می‌باشد.*

طرح برهان. بنابر قضیهٔ ۳.۳، R یک حاصل‌ضرب مستقیم (حلقه‌ای) ایده‌آلهای ساده است: $R = I_1 \times \cdots \times I_n$. بنابر سادگی، به‌ازای هر j، $I \cap I_j$ یا مساوی 0 است یا I_j. پس از اندیسگذاری مجدد در صورت لزوم، می‌توان فرض کرد که به‌ازای $j = 1, 2, \ldots, t$، $I \cap I_j = I_j$، و به‌ازای $j = t+1, \ldots, n$، $I \cap I_j = 0$. چون R طبق نتیجهٔ ۴.۳ یکدار است، $e_i \in I_i$ ای وجود دارد به‌طوری که $1_R = e_1 + e_2 + \cdots + e_n$. چون به‌ازای $j \neq k$، $I_j I_k = 0$، داریم

$$e_1 + e_2 + \cdots + e_n = 1_R = (1_R)^2 = e_1^2 + e_2^2 + \cdots + e_n^2,$$

که از آنجا، به‌ازای هر j، $e_j^2 = e_j$. به آسانی تحقیق می‌شود که هر e_i در مرکز R است و $e = e_1 + e_2 + \cdots + e_t$ خودتوانی در I است که در مرکز R می‌باشد. چون I ایده‌آل است، $Re \subset I$. به‌عکس، هرگاه $u \in I$، آنگاه $u = u1_R = ue_1 + \cdots + ue_n$. اما، به‌ازای $j > t$، $ue_j \in I \cap I_j = 0$. لذا، $u = ue_1 + \cdots + ue_t = ue$. بنابراین، $I \subset Re$.

قضیهٔ ۳.۳ توصیفی از حلقه‌های آرتینی چپ نیمه ساده با اصطلاحات نظریهٔ حلقه‌ها است. همانطورکه از رابطهٔ نزدیک حلقه‌ها و مدولها انتظار می‌رود، این حلقه‌ها را می‌توان فقط برحسب مدولها نیز توصیف کرد. برای به دست آوردن این توصیفها، به قضیه‌ای نیاز داریم که برای مدولهای روی یک حلقهٔ دلخواه معتبر باشد.

قضیهٔ ۶.۳. *شرایط زیر بر مدول ناصفر A روی حلقهٔ R باهم معادلند:*

(یک) A مجموع خانواده‌ای از زیرمدولهای ساده است؛

(دو) A مجموع مستقیم (داخلی) خانواده‌ای از زیرمدولهای ساده است؛

(سه) به‌ازای هر عنصر ناصفر a از A، $Ra \neq 0$؛ و هر زیرمدول B از A یک جمعوند مستقیم است (یعنی، به‌ازای زیرمدولی چون C، $A = B \oplus C$).

هر مدول صادق در شرایط معادل قضیهٔ ۶.۳ **نیمه ساده** یا ***کاملا*** " **تحویل‌ناپذیر** نام دارد. اصطلاح نیمه ساده از قضیهٔ ۳.۳ (دو) و این امر (ذیلا" ثابت می‌شود) که هر مدول روی یک حلقهٔ نیمه سادهٔ آرتینی (چپ) نیمه ساده است ناشی می‌شود.

طرح برهان ۶.۳. (دو) $\Rightarrow$ (یک) فرض کنیم A مجموع خانوادهٔ $\{B_i \mid i \in I\}$ از زیرمدولهای ساده باشد (یعنی، A به وسیلهٔ $\bigcup_{i\in I} B_i$ تولید می‌شود). با استفاده از لم زرن، نشان‌دهید که زیرمجموعه‌ای ناتهی مانند J از I وجود دارد که نسبت به خاصیت زیر ماکزیمال است: زیرمدول تولید شده به وسیلهٔ $\{B_j \mid j \in J\}$ درواقع یک مجموع مستقیم مانند $\sum_{j\in J} B_j$ می‌باشد. حکم می‌کنیم که $A = \sum_{j\in J} B_j$. برای اثبات این کافی است نشان دهیم که به‌ازای هر $i \in I$، $B_i \subset \sum_{j\in J} B_j$. چون B_i ساده‌بوده‌و $B_i \cap (\sum B_j)$ زیرمدولی از B_i است، یا $B_i \cap (\sum B_j) = B_i$ که‌ایجاب می‌کندکه $B_i \subset \sum B_j$، یا $B_i \cap (\sum B_j) = 0$.

حالت دوم نمی‌تواند رخ دهد. زیرا اگر رخ دهد، $K = \{i\} \cup J$ مجموعه‌ای خواهد بود که زیرمدول‌تولیدشده‌به‌وسیلهٔ $\{B_k \mid k \in K\}$ یک‌مجموع مستقیم است (قضیهٔ IV ۱۵.۱۰)، که ماکزیمالی J را نقض می‌کند.

(سه) $\Rightarrow$ (دو) فرض کنیم A مجموع‌مستقیم $\sum_{i\in I} B_i$ باشد، که‌درآن هر B_i یک زیرمدول ساده است. هرگاه a عنصر ناصفری از A باشد، آنگاه $a = b_{i_1} + \cdots + b_{i_k}$ که در آن $(i_1, \ldots, i_k \in I)$ $0 \neq b_{i_k} \in B_{i_k}$. واضح است که $Ra = 0$ اگر و فقط اگر به‌ازای هر i_k، $Rb_{i_k} = 0$. اما تبصرهٔ (سه) بعد از تعریف ۱.۱ نشان می‌دهد که $Rb_{i_k} = B_{i_k} \neq 0$. بنابراین: $Ra \neq 0$.

فرض کنیم B یک زیرمدول ناصفر A باشد. بنابر سادگی، $B \cap B_i$ یا 0 است یا B_i. هرگاه به‌ازای هر i، $B \cap B_i = B_i$، آنگاه $A = B$ و B بداهتا" یک جمعوند مستقیم است، $A = B \oplus 0$. درغیراین‌صورت، به‌ازای i ی، $B \cap B_i = 0$. با استفاده از لم زرن، زیرمجموعهٔ J از I را بیابید که نسبت به خاصیت زیر ماکزیمال باشد: $B \cap (\sum_{j\in J} B_j) = 0$. حکم می‌کنیم که $A = B \oplus (\sum_{j\in J} B_j)$. بنابر قضیهٔ IV ۱۵.۱۰، کافی است نشان دهیم که به‌ازای هر i، $B_i \subset B \oplus (\sum_{j\in J} B_j)$. هرگاه $i \in J$، آنگاه

$B_i \subset \sum_{j\in J} B_i$ و مطلب تمام است. هرگاه $i \notin J$ و $B_i \not\subset B \oplus \sum_{j\in J} B_j$، آنگاه، بنابر سادگی $B_i \cap (B \oplus \sum_{j\in J} B_j) = 0$. پس نتیجه می‌شود که $J \cup \{i\}$ مجموعه‌ای است که ماکزیمالی J را نقض می‌کند. بنابراین، $B_i \subset B \oplus \sum_{j\in J} B_j$.

(یک) $\Rightarrow$ (سه) ابتدا ملاحظه می‌کنیم که هرگاه N زیرمدولی از A باشد، آنگاه هر زیرمدول K از N یک جمعوند مستقیم N است. زیرا، طبق فرض، K یک جمعوند مستقیم A است؛ مثلا "، $A = K \oplus L$. تحقیق کنید که

$$N = N \cap A = (N \cap K) \oplus (N \cap L) = K \oplus (N \cap L).$$

حال نشان می‌دهیم که A دارای زیرمدولهای ساده است. چون $A \neq 0$، عنصر ناصفری مانند a از A وجوددارد. بااستفاده‌از لم زرن، زیرمدولی از A مانند B بیابید که نسبت به خاصیت $a \notin B$ ماکزیمال باشد. طبق فرض، به‌ازای زیرمدول ناصفری مانند C، $A = B \oplus C$ و $RC \neq 0$. حکم می‌کنیم که C ساده‌است. هرگاه ساده نباشد، آنگاه C دارای زیرمدولی حقیقی مانند D است، که بنابر بند پیش، یک جمعوند مستقیم C است. درنتیجه، $C = D \oplus E$ که $E \neq 0$، که ازآنجا $A = B \oplus C = B \oplus D \oplus E$، که در آن $D \neq 0$ و $E \neq 0$. اما $B \oplus D$ و $B \oplus E$ هر دوحقیقتا "شامل B است. بنابراین، طبق ماکزیمالی B، باید داشته باشیم $a \in B \oplus D$ و $a \in B \oplus E$. لذا، $b + d = a = b' + e$ $(b, b' \in B; d \in D; e \in E)$. اما

$$0 = a - a = (b - b') + d - e \in B \oplus D \oplus E$$

ایجاب می‌کند که $d = 0$، $e = 0$، و $b - b' = 0$. درنتیجه، $a = b \in B$، که تناقض است. بنابراین، C ساده می‌باشد.

فرض کنیم A_0 زیرمدولی از A باشدکه به وسیلهٔ تمام زیرمدولهای سادهٔ A تولید شده است. در این صورت، به‌ازای زیرمدولی چون N، $A = A_0 \oplus N$. بنابر بند پیش از آخرین بند، N در همان مفروضاتی صدق می‌کند که A در آنها صادق است. هرگاه $N \neq 0$، آنگاه استدلال بندپیش نشان می‌دهد که N شامل زیرمدول سادهٔ ناصفری مانند T است. چون T یک زیرمدول سادهٔ A است، $T \subset A_0$، لذا، $T \subset A_0 \cap N = 0$، که یک تناقض است. بنابراین، $N = 0$، که از آنجا $A = A_0$ مجموع خانواده‌ای از زیرمدولهای ساده می‌باشد.

حال می‌توان حلقه‌های آرتینی چپ نیمه ساده را به طرق مختلف برحسب مدولها توصیف کرد. چون زیرمدولهای حلقهٔ R (به عنوان یک R ــ مدول چپ) دقیقاً" ایده‌آلهای چپ R اند، بعضی از این توصیفها برحسب ایده‌آلهای چپ بیان شده‌اند. زیرمجموعهٔ $\{e_1, \ldots, e_m\}$ از R مجموعه‌ای‌از ***خودتوانهای متعامد*** است اگر به‌ازای هر i ، $e_i^2 = e_i$ و به‌ازای هر $i \neq j$ ، $e_ie_j = 0$.

قضیهٔ ۷.۳ . شرایط زیر بر حلقهٔ ناصفر و یکدار R با هم معادلند :

(یک) R آرتینی چپ نیمه ساده است ؛

(دو) هر R ــ مدول چپ یکانی تصویری است ؛

(سه) هر R ــ مدول چپ یکانی انژکتیو است ؛

(چهار) هر دنبالهٔ کامل کوتاه از R ــ مدولهای چپ یکانی کامل تجزیه است ؛

(پنج) هر R ــ مدول چپ یکانی ناصفر نیمه ساده است ؛

(شش) R خود یک R ــ مدول چپ نیمه سادهٔ یکانی است ؛

(هفت) هر ایده‌آل چپ R به شکل Re است ، که در آن e خودتوان می‌باشد ؛

(هشت) R مجموع مستقیم (داخلی) (به عنوان یک R ــ مدول چپ) ایده‌آلهای چپ مینیمال $K_1, \ldots, K_m$ است به‌طوری که به‌ازای $(e_i \in R)$ $K_i = Re_i$ ، $i = 1,2, \ldots, m$ و $e_1 + e_2 + \cdots + e_m = 1_R$ که $\{e_1, \ldots, e_m\}$ مجموعه‌ای از خودتوانهای متعامد است .

چند تبصره . چون یک حلقهٔ نیمه ساده آرتینی چپ است اگر و فقط اگر آرتینی راست باشد (نتیجهٔ ۴.۳)، هریک ازشرایط قضیهٔ ۷.۳ بامشابه واضح‌خود برای مدولهای راست یا ایده‌آلهای‌راست‌معادل است . فرض یکدار بودن R خللی به کلیت وارد نمی‌آورد ، زیرا ، بنابر نتیجهٔ ۴.۳ ، هر حلقهٔ آرتینی‌چپ‌نیمه ساده لزوما" یکدار است . قضیه درصورت حذف کلمهٔ "یکانی" درست نیست (تمرین ۱۰) .

طرح برهان ۷.۳ . (چهار) $\Leftrightarrow$ (سه) $\Leftrightarrow$ (دو) تمرین IV ۱.۳۰ است . برای اتمام برهان ، استلزامهای (پنج) $\Leftrightarrow$ (چهار) و

(پنج) $\Rightarrow$ (هشت) $\Rightarrow$ (یک) $\Rightarrow$ (شش) $\Rightarrow$ (هفت) $\Rightarrow$ (پنج) را ثابت می‌کنیم .

(پنج) $\Rightarrow$ (چهار) هرگاه B زیرمدولی از R ــ مدول یکانی و ناصفر A باشد ، آنگاه

$$0 \to B \xrightarrow{\subseteq} A \to A/B \to 0$$

یک دنبالهٔ کامل کوتاه است، که طبق فرض تجزیه می‌شود. برهان قضیهٔ IV ۱۸۰۱۰ نشان می‌دهد که $A = B \oplus C$ که در آن $C \cong A/B$. چون A یکانی است، به‌ازای هر عنصر ناصفر $a \in A$، $Ra \neq 0$. بنابراین، طبق قضیهٔ ۶۰۳، A نیمه ساده است.

(چهار) $\Rightarrow$ (پنج) فرض کنیم $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ یک دنبالهٔ کامل کوتاه از R ــ مدولهای یکانی باشد. در این صورت، $f : A \to f(A)$ یکریختی است. چون B بنابر (پنج) نیمه ساده است، $f(A)$ طبق قضیهٔ ۶۰۳ یک جمعوند مستقیم B می‌باشد. هرگاه $\pi : B \to f(A)$ برو‌ریختی کانونی باشد، آنگاه $\pi f = f$ و $f^{-1}\pi : B \to A$ یک همریختی R ــ مدولهاست به‌طوری که $(f^{-1}\pi)f = 1_A$. بنابراین، طبق قضیهٔ IV ۱۸۰۱۰، دنباله تجزیه می‌شود.

(هفت) $\Rightarrow$ (پنج) ایده‌آلهای چپ R دقیقا" زیرمدولهای آن می‌باشند. هرگاه L یک ایده‌آل چپ باشد، آنگاه، بنابر (پنج) و قضیهٔ ۶۰۳، به‌ازای ایده‌آلی چپ چون I، $R = L \oplus I$. درنتیجه، عناصری چون $e_1 \in L$ و $e_2 \in I$ وجود دارند به طوری که $1_R = e_1 + e_2$. چون $e_1 \in L$، $Re_1 \subset L$. هرگاه $r \in L$، آنگاه $r = re_1 + re_2$، که از آنجا $re_2 = r - re_1 \in L \cap I = 0$. لذا، به‌ازای هر $r \in L$، $r = re_1$؛ بخصوص، $e_1e_1 = e_1$ و $L \subset Re_1$. بنابراین، $L = Re_1$، که در آن e_1 خودتوان است.

(شش) $\Rightarrow$ (هفت) یک زیرمدول R مانند L ایده‌آل چپ است؛ درنتیجه، $L = Re$ که در آن e خودتوان است. تحقیق کنید که $R(1_R - e)$ ایده‌آلی چپ از R است به‌طوری که $R = Re \oplus R(1_R - e)$. بنابراین، طبق قضیهٔ ۶۰۳، R نیمه ساده می‌باشد.

(یک) $\Rightarrow$ (شش) طبق فرض، R مجموع مستقیمی مانند $\sum_{i \in I} B_i$ است، که در آن هر B_i یک زیرمدول ساده (ایده‌آل چپ) R است. درنتیجه، زیرمجموعه‌ای متناهی از I_0 مانند I وجود دارد (که عناصرش برای راحتی برچسب $1, 2, \ldots, k$ خورده‌اند) به‌طوری که $1_R = e_1 + e_2 + \cdots + e_k$ $(e_i \in B_i)$. لذا، به‌ازای هر $r \in R$،

$$r = re_1 + re_2 + \cdots + re_k \in \sum_{i=1}^{k} B_i,$$

که از آنجا $R = \sum_{i=1}^{k} B_i$. هرگاه $r \in J(R)$، آنگاه، بنابر قضیهٔ ۳۰۲ (یک)، به‌ازای هر

$rB_i = 0$ ، i . درنتیجه ،

$$r = r1_R = re_1 + re_2 + \cdots + re_k = 0.$$

بنابراین ، $J(R) = 0$ و R نیمه ساده است . چون B_i ساده است و

$$(B_1 \oplus \cdots \oplus B_i)/(B_1 \oplus \cdots \oplus B_{i-1}) \cong B_i,$$

سری

$$R = B_1 \oplus \cdots \oplus B_k \supset B_1 \oplus \cdots \oplus B_{k-1} \supset \cdots \supset B_1 \oplus B_2 \supset B_1 \supset 0$$

یک سری ترکیبی برای R است . بنابراین ، طبق قضیهٔ VIII ۱۱.۱۰ ، R آرتینی چپ است .

(هشت) $\Rightarrow$ (یک) در پرتو قضیهٔ ۳.۳ ، کافی است فرض کنیم $R = \prod_{i=1}^{t} \mathrm{Mat}_{n_i} D_i$ ، که در آن هر $n_i > 0$ و هر D_i یک حلقهٔ بخشی است . فرض کنیم به‌ازای هر i ثابت و هر $j = 1, 2, \ldots, n_i$ ، e_{ij} ماتریسی در $\mathrm{Mat}_{n_i} D_i$ باشد که در موضع (j,j) آن 1_{D_i} و در جاهای دیگر 0 است . در این صورت ، $\{e_{i1}, \ldots, e_{in_i}\}$ مجموعه‌ای از خودتوانهای متعامد در $\mathrm{Mat}_{n_i} D_i = R_i$ است که مجموعشان ماتریس همانی می‌باشد . برهان نتیجهٔ VIII ۱۲.۱۰ نشان می‌دهد که هر $R_i e_{ij}$ یک ایده‌آل چپ مینیمال R_i است و $R_i = R_i e_{i1} \oplus \cdots \oplus R_i e_{in_i}$. چون R حلقهٔ حاصلضرب مستقیم $R_1 \times \cdots \times R_t$ است ، نتیجه می‌شود که به‌ازای $i \neq j$ ، $R_i R_j = 0$ ؛ $Re_{ij} = R_i e_{ij}$ ؛ Re_{ij} یک ایده‌آل چپ مینیمال R است ؛ و

$$\{e_{ij} \mid 1 \leq i \leq t;\ 1 \leq j \leq n_i\}$$

مجموعه‌ای از خودتوانهای متعامد در R است که مجموعشان مساوی است با

$$\sum_{i=1}^{t} (\sum_{j} e_{ij}) = \sum_{i=1}^{t} 1_{R_i} = 1_R.$$

واضح است که $R = \sum_{i=1}^{t} \sum_{j=1}^{n_i} Re_{ij}$.

(پنج) $\Rightarrow$ (هشت) فرض کنیم A یک R ــ مدول یکانی باشد . به‌ازای هر $a \in A$ و هر i ، $K_i a$ زیرمدولی از A است (تمرین IV ۳.۱۰) و

$$a = 1_R a = e_1 a + \cdots + e_m a \in K_1 a + \cdots + K_m a.$$

درنتیجه ، زیرمدولهای $K_i a$ $(a \in A,\ 1 \leq i \leq m)$ A را تولید می‌کنند . به‌ازای هر $a \in A$ و هر i ، نگاشت $f : K_i \to K_i a$ داده شده با $k \mapsto ka$ یک بروریختی R ــ مدولهاست .

چون K_i یک‌ایده‌آل‌چپ‌مینیمال حلقه‌ای یکدار است، K_i یک R ــ مدول ساده می‌باشد. درنتیجه، هرگاه $K_ia \neq 0$، آنگاه، طبق لم ۱۰.۱ شور، f یکریختی است. لذا، $\{K_ia \mid 1 \leq i \leq m; a \in A; K_ia \neq 0\}$ خانواده‌ای از زیرمدولهای ساده است که مجموعشان مساوی A می‌باشد. بنابراین، طبق قضیهٔ ۶.۳، A نیمه ساده می‌باشد.

قضایای ۳.۳ و ۷.۳ نشان می‌دهند که یک حلقهٔ آرتینی چپ نیمه ساده را می‌توان به صورت حاصلضرب [مجموع] مستقیمی از ایده‌آلهای ساده [ایده‌آلهای چپ مینیمال] تجزیه کرد. حال به یکتایی این ترکیبات می‌پردازیم.

حکم ۸.۳. *فرض کنیم R یک حلقهٔ آرتینی چپ نیمه ساده باشد.*
(یک) $R = I_1 \times \cdots \times I_n$، که در آن I_j یک ایده‌آل سادهٔ R است.
(دو) هرگاه J ایده‌آل ساده‌ای از R باشد، آنگاه، به‌ازای k ای، $J = I_k$.
(سه) هرگاه $R = J_1 \times \cdots \times J_m$ که در آن هر J_k ایده‌آل ساده‌ای از R است، آنگاه $n = m$ و (پس از اندیسگذاری مجدد) به‌ازای $k = 1,2,\ldots,n$، $I_k = J_k$.

چند تبصره. نتیجهٔ "$J = I_j$ [یا $J_k = I_k$]" خیلی از حکم "J [یا J_k] با I_k یکریخت است" قویترمی‌باشد. ایده‌آلهای سادهٔ منحصر به فرد $I_1, \ldots, I_n$ در حکم ۸.۳ ***مؤلفه‌های سادهٔ R*** نام دارند.

برهان ۸.۳. (یک) طبق قضیهٔ ۳.۳ برقرار است. (دو) هرگاه J ایده‌آل ساده‌ای از R باشد، آنگاه $RJ \neq 0$؛ درنتیجه، به‌ازای k ای، $I_kJ \neq 0$. چون I_kJ ایده‌آل ناصفری است که مشمول هر دوی I_k و J است، سادگی I_k و J ایجاب می‌کند که $I_k = I_kJ = J$. (سه) ایده‌آلهای $I_1, \ldots, I_n$ [$J_1, \ldots, J_m$] طبق فرض ناصفر و دو بدو ازهم جدایند. نگاشت θ را از مجموعهٔ m عنصری $\{J_1, \ldots, J_m\}$ به مجموعهٔ n عنصری $\{I_1, \ldots, I_n\}$ با $J_k \mapsto I_k$ تعریف می‌کنیم، که در آن $J_k = I_k$. طبق (دو)، θ تعریف شده و انژکتیو است، که از آنجا $m \leq n$. همین استدلال که در آن نقشهای J_k و I_k با هم عوض شده‌اند نشان می‌دهد که $n \leq m$. بنابراین، $n = m$ و θ بیژکسیون می‌باشد.

بنابر قضیهٔ ۷.۳ (هشت)، حلقهٔ آرتینی چپ نیمه سادهٔ R مجموع مستقیمی از ایده‌آلهای چپ مینیمال است. یکتایی (با تقریب یکریختی) این تجزیه نتیجهٔ فوری حکم زیراست. زیرا R یک R ــ مدول نیمه ساده بوده (قضیهٔ ۷.۳ (شش)) و ایده‌آلهای چپ مینیمال R دقیقاً" زیرمدولهای سادهٔ آن می‌باشند.

حکم ۹.۳ . *فرض کنیم A یک مدول نیمه ساده روی حلقهٔ R باشد. هرگاه تجزیه‌های مجموع مستقیم*

$$A = C_1 \oplus \cdots \oplus C_n \quad \text{و} \quad A = B_1 \oplus \cdots \oplus B_m$$

موجود باشند، که در آنها هر B_i, C_j زیرمدول ساده‌ای از A باشد، آنگاه $m = n$ و (پس از اندیسگذاری مجدد) به‌ازای $i = 1,2,\ldots,m$ ، $B_i \cong C_i$.

تبصره. در اینجا حکم یکتایی از یکتایی مذکور در حکم ۸.۳ ضعیفتر است. حکم ۹.۳ در صورت تعویض "$B_i \cong C_i$" با "$B_i = C_i$" درست نیست (تمرین ۱۱).

برهان ۹.۳ . سری

$$A = B_1 \oplus \cdots \oplus B_m \supset B_2 \oplus \cdots \oplus B_m \supset \cdots \supset B_m \supset 0$$

یک سری‌ترکیبی‌برای A با عوامل سادهٔ $B_1, B_2, \ldots, B_m$ است (ر.ک. ص ۵۸۴). به همین نحو، $A = C_1 \oplus \cdots \oplus C_n \supset C_2 \oplus \cdots \oplus C_m \supset \cdots \supset C_m \supset 0$ یک سری ترکیبی برای A با عوامل سادهٔ $C_1, \ldots, C_n$ می‌باشد. قضیهٔ ژردان ــ هولدر VIII ۱۰.۱۰ ایجاب می‌کند که $m = n$ و (پس از اندیسگذاری مجدد) به‌ازای $i = 1,2,\ldots,m$ ، $B_i \cong C_i$.

قضیهٔ زیر فقط در برهان قضیهٔ ۷.۶ به کار خواهد رفت.

قضیهٔ ۱۰.۳ . *فرض کنیم R یک حلقهٔ آرتینی چپ نیمه ساده باشد.*

(یک) هر R ــ مدول‌چپ [راست] ساده با یک ایده‌آل‌چپ [راست] مینیمال R یکریخت است.

(دو) تعداد R ــ مدولهای چپ [راست] سادهٔ غیریکریخت مساوی تعداد مولفه‌های سادهٔ R است.

برهان. بنابر نتیجهٔ ۴.۳ ، R آرتینی راست است. چون نتایج قبل متقارن چپ ــ راست‌اند ، کافی است قضیه را برای مدولهای چپ ثابت نماییم.

(یک) بنابر قضیهٔ ۷.۳ ، $R = K_1 \oplus \cdots \oplus K_m$ که‌درآن‌هر K_i یک‌ایده‌آل چپ مینیمال ناصفر (زیرمدول سادهٔ R) R است. R یکدار است (نتیجهٔ ۴.۳) و ، بنابر تبصرهٔ (دو) بعد از تعریف ۱.۱ ، هر R ــ مدول سادهٔ A یکانی است. برهان (پنج) $\Rightarrow$ (هشت) قضیهٔ ۷.۳ نشان می‌دهد که به‌ازای i ی $(1 \leq i \leq m)$ و $a \in A$ ای ، A شامل زیرمدول ناصفر $K_i a$ است به‌طوری که $K_i a \cong K_i$. سادگی A ایجاب می‌کند که $A = K_i a \cong K_i$.

(دو) مولفه‌های سادهٔ R ایده‌آلهای سادهٔ منحصر به فرد I_i از R هستند به‌طوری که $R = I_1 \times \cdots \times I_n$ (حکم ۸.۳) . در پرتو قسمت (یک) کافی است ثابت کنیم

(آ) هر K_i مشمول I_t ای است؛

(ب) هر I_t شامل K_i ی است؛

(پ) به عنوان R ــ مدول $K_i \cong K_j$ اگرو فقط‌اگر K_i و K_j مشمول مولفهٔ سادهٔ یک I_t باشند.

این احکام به‌صورت زیر ثابت می‌شوند.

(آ) چون R یکدار است ، $K_i = RK_i = I_1K_i \times \cdots \times I_nK_i$. چون هر I_jK_i یک ایده‌آل چپ R مشمول K_i است ، باید بنابر مینیمالی به‌ازای t ای داشته باشیم $I_tK_i = K_i$ و به‌ازای $j \neq t$ داشته باشیم $I_jK_i = 0$. بنابراین ، $K_i = I_tK_i \subset I_t$.

(ب) هرگاه I_t شامل K_i ی نباشد ، آنگاه ، بنابر (آ) ، $R = \sum K_i$ مشمول

$$I_1 \times \cdots \times I_{t-1} \times 0 \times I_{t+1} \times \cdots \times I_n$$

می‌باشد . چون بنابر سادگی $I_t \neq 0$ و $R = \prod I_i$ ،

$$0 \neq I_t = I_t \cap R = I_t \cap (I_1 \times \cdots \times I_{t-1} \times I_{t+1} \times \cdots \times I_n) = 0,$$

که تناقض است.

(پ) هرگاه $K_i \subset I_{t_1}$ و $K_j \subset I_{t_2}$ که $t_1 \neq t_2$ ، آنگاه ، بنابر (آ) ، $0 \neq K_i = I_{t_1}K_i$ و $0 \neq K_j = I_{t_2}K_j$. چون $R = \prod I_i$ ، داریم $I_{t_1}I_{t_2} = 0 = I_{t_2}I_{t_1}$. درنتیجه ، نمی‌تواند یکریختی R ــ مدولهای $K_i \cong K_j$ وجود داشته باشد . به عکس، فرض کنیم $K_i \subset I_t$ و

$K_i \subset I_t$. در این صورت، K_i و K_i ، I_t ــ مدول می‌باشند. چون، بنابر (آ) ، I_t ساده بوده و $0 \neq K_i = I_t K_i$ ، ایده‌آل صفرساز چپ K_i در I_t باید صفر باشد. درنتیجه، $K_i K_i \neq 0$ زیرا $0 \neq K_i \subset I_t$. لذا، به‌ازای $a \in K_i$ ای، $K_i a \neq 0$. چون K_i و K_i ایده‌آلهای چپ R اند، $K_i a$ یک ایده‌آل چپ ناصفر R بوده و $K_i a \subset K_i$. بنابراین، طبق مینیمالی، $K_i a = K_i$. برهان (پنج) $\Rightarrow$ (هشت) قضیهٔ ۷.۳ نشان می‌دهد که $K_i a \cong K_i$ ، که از آنجا $K_i \cong K_i$.

تمرینات

۱ . حلقهٔ R با حاصلضرب‌زیرمستقیمی‌ازخانوادهٔ $\{R_i \mid i \in I\}$ از حلقه‌ها یکریخت است اگر و فقط اگر به‌ازای هر $i \in I$ ایده‌آلی مانند K_i از R موجود باشد به‌طوری که $R/K_i \cong R_i$ و $\bigcap_{i \in I} K_i = 0$.

۲ . حلقهٔ R **به‌طور زیرمستقیم تحویل‌ناپذیر** است اگر اشتراک تمام ایده‌آلهای ناصفر R ناصفر باشد.

(آ) R به‌طور زیرمستقیم تحویل‌ناپذیر است اگر و فقط اگر هر وقت R با حاصلضرب زیرمستقیمی از $\{R_i \mid i \in I\}$ یکریخت باشد، به‌ازای $i \in I$ ی، $R \cong R_i$ [ر.ک. تمرین ۱] .

(ب) (بیرکف[1]) هرحلقه‌باحاصلضرب‌زیرمستقیمی‌ازیک خانوادهٔ به‌طور زیرمستقیم تحویل‌ناپذیر از حلقه‌ها یکریخت است.

(پ) مقسوم‌علیه‌های صفر (به انضمام 0) در یک حلقهٔ تعویضپذیر که به‌طور زیرمستقیم تحویل‌ناپذیر است یک ایده‌آل تشکیل می‌دهند.

۳ . یک حلقهٔ آرتینی چپ نیمه سادهٔ تعویضپذیر حاصلضرب مستقیمی از میدانهاست.

۴ . تمام حلقه‌های نیمه ساده از مرتبهٔ 1008 را با تقریب یکریختی تعیین کنید. چند تا از آنها تعویضپذیرند؟ [**راهنمایی** . تمرین ۷.۸۰۱۰ .]

۵ . عنصر a از حلقهٔ R **منتظم** (به مفهوم فون‌نویمان[2]) است اگر $x \in R$ ی باشد به طوری که $axa = a$. هرگاه هر عنصر R منتظم باشد، آنگاه گوییم R یک **حلقهٔ منتظم** است.

---

1. Birkhoff 2. Von Neumann

(آ) هر حلقهٔ بخشی منتظم است.
(ب) هر حاصل‌ضرب مستقیم متناهی از حلقه‌های منتظم منتظم است.
(پ) هرحلقهٔ‌منتظم نیمه‌ساده‌است. [عکس مطلب‌درست‌نیست (مثلا " $\mathbf{Z}$ ، $\mathbf{Z}$) .]
(ت) حلقهٔ تمام تبدیلات خطی بر یک فضای برداری (نه لزوما" با بعد متناهی) روی یک حلقهٔ بخشی منتظم است.
(ث) یک حلقهٔ آرتینی چپ نیمه ساده منتظم است.
(ج) R منتظم است اگر و فقط‌اگر هر ایده‌آل اصلی چپ [راست] R به وسیلهٔ یک عنصر خودتوان تولید شده باشد.
(چ) حلقهٔ منتظم ناصفر و یکدار R یک حلقهٔ بخشی است اگر و فقط‌اگر خودتوانهای آن منحصر به 0 و 1_R باشند.

۶. (آ) هر نقش‌همریخت ناصفر و هر زیرمدول ناصفر یک مدول نیمه ساده نیمه ساده است.
(ب) اشتراک دو زیرمدول نیمه ساده 0 یا نیمه ساده است.

۷. شرایط‌زیر بر مدول نیمه سادهٔ A باهم معادلند:
(آ) A با تولید متناهی است؛
(ب) A مجموع مستقیمی از تعدادی متناهی زیرمدول ساده است؛
(پ) A دارای سری ترکیبی می‌باشد (ر.ک. ص ۵۸۴)؛
(ت) A در هر دو شرط زنجیر افزایشی و کاهشی بر زیرمدولها صدق می‌کند (ر.ک. قضیهٔ VIII ۱۱.۱۰).

۸. فرض‌کنید A یک مدول روی حلقهٔ آرتینی چپ R باشد به‌طوری که به‌ازای هر $a \in A$ ی ناصفر، $Ra \neq 0$ و نیز $J = J(R)$. در این صورت، $JA = 0$ اگر و فقط‌اگر A نیمه‌ساده‌باشد. [**راهنماییها.** هرگاه $JA = 0$ ، آنگاه A یک R/J ــ مدول است، که‌درآن R/J آرتینی‌چپ‌نیمه ساده می‌باشد؛ ر.ک. تمرین IV ۱۷.۱۰ .]

۹. فرض‌کنید R حلقه‌ای باشد که (به عنوان یک R ــ مدول چپ) مجموع ایده‌آلهای چپ مینیمال‌آن‌است. همچنین، $\{r \in R \mid Rr = 0\} = 0$. هرگاه A یک R ــ مدول باشد به‌طوری که $RA = A$ ، آنگاه A نیمه‌ساده‌است. [**راهنمایی.** اگر I یک ایده‌آل چپ مینیمال بوده و $a \in A$ ، نشان دهید که Ia یا صفر است یا زیرمدول ساده‌ای از A می‌باشد.]

۱۰ . نشان دهید که R ــ مدول‌ناصفر A باخاصیت $RA = 0$ نیمه‌ساده نیست ولی ممکن است تصویری باشد . درنتیجه ، قضیهٔ ۷۰۳ در صورت حذف لغت "یکانی" ممکن است درست نباشد . [ر.ک. تمرین IV ۲۰۲۰ ، قضیهٔ IV ۲۰۳۰ ، و حکم IV ۰۵۰۳۰]

۱۱ . فرض کنید R حلقهٔ ماتریسهای 2×2 روی یک میدان نامتناهی باشد .

(آ) R دارای تعدادی نامتناهی ایده‌آل چپ حقیقی متمایز است که هر دو تا به عنوان R ــ مدول چپ باهم یکریخت‌اند .

(ب) بی‌نهایت‌جفت‌متمایزمانند (B,C) وجوددارند به‌طوری که B و C ایده‌آلهای چپ مینیمال R بوده و $R = B \oplus C$.

۱۲ . تعداد R ــ مدولهای چپ سادهٔ غیریکریخت حلقهٔ آرتینی چپ R با تعداد R ــ مدولهای راست سادهٔ غیر یکریخت آن برابر است . [**راهنمایی .** نشان دهید A یک R ــ مدول‌ساده‌است‌اگرو فقط‌اگر A یک $R/J(R)$ ــ مدول ساده باشد ؛ از قضیهٔ ۱۴۰۲ و قضیهٔ ۱۰۰۳ استفاده کنید .]

۱۳ . (آ) (هاپکینز[1]) هرگاه R یک حلقهٔ یکدار آرتینی چپ باشد ، آنگاه R نوتری چپ است . [**راهنماییها :** فرض کنید n کوچکترین عدد صحیح مثبتی باشد که $J^n = 0$ (حکم ۱۳۰۲) . قراردهید $J^0 = R$. چون $J(J^i/J^{i+1}) = 0$ و J^i/J^{i+1} آرتینی چپ می‌باشد ، بنابر تمرینهای ۷ و ۸ ، هر J^i/J^{i+1} $(0 \leq i \leq n-1)$ دارای سری ترکیبی است . بااستفاده ازاینها و قضیهٔ IV ۱۰۰۱۰ ، یک سری ترکیبی برای R بسازید ؛ قضیهٔ VIII ۱۱۰۱۰ را به کار برید .

[**تبصره .** اگر فرض "یکدار بودن R" با فرض بسیار ضعیفتر $rR = 0$ و $Rr = 0 \mid r \in R\}$ = 0 عوض شود ، بازهم قضیهٔ هاپکینز برقرار است ؛ ر.ک. ال. فوکس [۱۳ ؛ صفحات ۲۸۳ تا ۲۸۶] .

(ب) عکس قضیهٔ هاپکینز درست نیست .

۴ رادیکال اول ؛ حلقه‌های اول و نیمه اول

حال رادیکال اول یک حلقه را معرفی کرده و یک حلقه را نیمه اول نامیم اگر دارای رادیکال

1. Hopkins

اول صفر باشد (تعریف ۱۰۴) . سپس نتایجی مشابه نتایج ثابت شده در بخشهای ۲ و ۳ برای رادیکال ژاکوبسون‌وحلقه‌های‌نیمه ساده را اثبات می‌نماییم (احکام ۲۰۴ تا ۴۰۴) . تشابهی‌قوی به‌ترتیب بین رادیکال‌اول ،ایده‌آلهای اول ، حلقه‌های نیمه ساده ، حلقه‌های اول ، و رادیکال ژاکوبسون ، ایده‌آلهای اولیهٔ چپ ، حلقه‌های نیمه ساده ، و حلقه‌های اولیه وجود دارد .

تا پایان این بخش به قضیهٔ گولدی ۸۰۴ اختصاص دارد ، که یک قضیهٔ ساختاری برای حلقه‌های نیمه اولی است که در شرط‌زنجیر افزایشی بر انواع خاصی از ایده‌آلهای چپ صدق می‌کنند . قضیهٔ گولدی همان نقشی را در اینجا دارد که قضایای ودربورن ـ آرتین ۱۴۰۱ و ۳۰۳ در حلقه‌ها با شرط زنجیر افزایشی بر ایده‌آلهای چپ دارند . درواقع ، قضیهٔ گولدی را می‌توان تعمیمی از قضایای ودربورن ـ آرتین به ردهٔ وسیعتری ازحلقه‌ها درنظرگرفت . توضیح‌کاملتر این احکام بعد از حکم ۴۰۴ ، قبل از قضیهٔ ۸۰۴ ، و بعد از نتیجهٔ ۹۰۴ داده شده است .

این بخش در آینده به کار نخواهد آمد .

تعریف ۱۰۴ . ***رادیکال اول*** $P(R)$ از حلقهٔ R اشتراک تمام ایده‌آلهای اول R است . هرگاه R ایده‌آل اول نداشته باشد ، آنگاه $P(R) = R$. حلقهٔ R با خاصیت $P(R) = 0$ ***نیمه اول*** نام دارد .

چند تبصره . رادیکال اول (که ***رادیکال پایینی بائر***[1] یا ***رادیکال مک‌کوی***[2] نیز نام دارد) رادیکالی است نسبت به یک خاصیت رادیکال مشخص، به صورت تعریف شده در مقدمهٔ بخش ۲ ؛ برای جزئیات ، ر.ک. تمرینات ۱ و ۲ . یک حلقهٔ نیمه اول حلقه‌ای است که نسبت به رادیکال اول نیمه ساده باشد (ر.ک. مقدمهٔ بخش ۲) . برای احتراز از اشتباه با اصطلاح نامطلوب‌نیمه‌سادگی‌ژاکوبسون ، از واژهٔ "نیمه اول" استفاده می‌کنیم . رابطهٔ رادیکال اول با رادیکال ژاکوبسون در تمرین ۳ مطرح شده است .

درست مثل رادیکال ژاکوبسون ، رابطهٔ نزدیکی بین رادیکال اول حلقهٔ R و ایده‌آلهای‌پوچ‌توان R وجوددارد . برای اثبات یک چنین نتیجه ، چند اصطلاح را یادآور می‌شویم .

---

1. Baer ,
2. MeCoy

فرض کنیم S زیرمجموعه‌ای از حلقهٔ R باشد. بنابر قضیهٔ ۴.۱، مجموعهٔ $\{r \in R \mid rS = 0\}$ یک ایده‌آل چپ R است، که در صورت ایده‌آل چپ بودن S یک ایده‌آل است. مجموعهٔ $\{r \in R \mid rS = 0\}$ **صفرساز چپ** S نام دارد و با $\mathfrak{A}(S)$ نموده می‌شود. به همین نحو، مجموعهٔ

$$\mathfrak{A}_r(S) = \{r \in R \mid Sr = 0\}$$

یک ایده‌آل راست R است که در صورت ایده‌آل راست بودن S ایده‌آل می‌باشد. $\mathfrak{A}_r(S)$ **صفرساز راست** S نام دارد. ایده‌آل چپ [راست] I از R را یک صفرساز چپ [راست] نامند اگر به‌ازای زیرمجموعه‌ای از R مانند S، $I = \mathfrak{A}(S)$ [$I = \mathfrak{A}_r(S)$].

تبصره. اشتراک دو صفرساز چپ [راست] یک صفرساز چپ [راست] است، زیرا $\mathfrak{A}(S) \cap \mathfrak{A}(T) = \mathfrak{A}(S \cup T)$. هرگاه S و T ایده‌آلهای چپ باشند، آنگاه

$$\mathfrak{A}(S) \cap \mathfrak{A}(T) = \mathfrak{A}(S \cup T) = \mathfrak{A}(S + T).$$

حکم ۲.۴. *حلقهٔ R نیمه‌اول است اگر و فقط اگر R ایده‌آل پوچ‌توان ناصفر نداشته باشد.*

طرح برهان. ($\Leftarrow$) هرگاه I ایده‌آل پوچ‌توانی بوده و K ایده‌آل اول دلخواهی باشد، آنگاه، به‌ازای n ی، $I^n = 0 \in K$، که از آنجا $I \subset K$. بنابراین، $I \subset P(R)$. درنتیجه، هرگاه R نیمه‌اول باشد، یعنی $P(R) = 0$، آنگاه تنها ایده‌آل پوچ‌توان ایده‌آل صفر است.
($\Rightarrow$) به عکس، فرض کنیم R ایده‌آل پوچ‌توان ناصفر نداشته باشد. باید نشان دهیم که $P(R) = 0$. کافی است ثابت کنیم به‌ازای هر عنصر ناصفر a از R، یک ایده‌آل اول مانند K وجود دارد به‌طوری که $a \notin K$، که از آنجا $a \notin P(R)$. ابتدا ملاحظه می‌کنیم که $\mathfrak{A}(R) \cap R$ یک ایده‌آل پوچ‌توان R است، زیرا

$$(\mathfrak{A}(R) \cap R)(\mathfrak{A}(R) \cap R) \subset \mathfrak{A}(R)R = 0.$$

درنتیجه، $\mathfrak{A}(R) = \mathfrak{A}(R) \cap R = 0$. به همین نحو، $\mathfrak{A}_r(R) = 0$. اگر b عنصر ناصفری از R باشد، حکم می‌کنیم $RbR \neq 0$. درغیر این صورت، $Rb \subset \mathfrak{A}(R) = 0$، که از آنجا $Rb = 0$. لذا، $b \in \mathfrak{A}_r(R) = 0$، که یک تناقض است. بنابراین، KbR ایده‌آل ناصفری از R است؛ و لذا، پوچ‌توان نیست. درنتیجه، $bRb \neq 0$ (در غیر این صورت، $(RbR)^2 \subset RbRbR = 0$). به‌ازای هر عنصر ناصفر $b \in R$، $f(b) \in bRb$ را طوری اختیار

می‌کنیم که $f(b) \neq 0$. دراین‌صورت ، بنابر قضیهٔ بازگشتی ۲.۶ در آشنایی ،تابعی مانند $\varphi : \mathbf{N} \to R$ وجود دارد به‌طوری که

$$\varphi(0) = a \quad \text{و} \quad \varphi(n+1) = f(\varphi(n)) \ .$$

فرض کنیم $a_n = \varphi(n)$ ؛ درنتیجه ، $a_{n+1} = f(a_n) \neq 0$. همچنین ، $S = \{a_i \mid i \geq 0\}$. با استفاده ازلم‌زرن ، ایده‌آلی مانند K بیابید که نسبت به خاصیت $K \cap S = \varnothing$ ماکزیمال باشد (چون $0 \notin S$ ، دست‌کم یک ایده‌آل جدا از S وجود دارد) .

چون $a = a_0 \in S$ ، داریم $a \notin K$ و $K \neq R$. برای اتمام برهان ، کافی است نشان دهیم که K اول است . هرگاه A و B ایده‌آلهایی از R باشند به‌طوری که $A \not\subset K$ و $B \not\subset K$ ، آنگاه ، بنابر ماکزیمالی ، $(A+K) \cap S \neq \varnothing$ و $(B+K) \cap S \neq \varnothing$. درنتیجه ، به‌ازای i,j ای ، $a_i \in A + K$ و $a_j \in B + K$. $m > \max\{i,j\}$ را اختیار می‌کنیم . چون به‌ازای هر n ، $a_{n+1} = f(a_n) \in a_n R a_n$ ، نتیجه می‌شود که

$$a_m \in (a_i R a_i) \cap (a_j R a_j) \subset (A+K) \cap (B+K).$$

درنتیجه ،

$$a_{m+1} = f(a_m) \in a_m R a_m \subset (A+K)(B+K) \subset AB + K.$$

چون $a_{m+1} \notin K$ ، باید داشته باشیم $AB \not\subset K$. بنابراین ، K یک ایده‌آل اول می‌باشد .

گوییم حلقهٔ R یک *حلقهٔ اول* است اگر ایده‌آل صفر یک ایده‌آل اول باشد (یعنی ، هرگاه I, J ایده‌آلهایی باشند به‌طوری که $IJ = 0$ ، آنگاه $I = 0$ یا $J = 0$) . روابط بین ایده‌آلهای اول ، حلقه‌های اول ، و حلقه‌های نیمه اول شبیه روابط بین ایده‌آلهای اولیهٔ چپ ، حلقه‌های اولیه ، و حلقه‌های نیمه ساده است . بخصوص ، نکات زیر قابل توجه می‌باشند :

(یک) رادیکال اول [ژاکوبسون] اشتراک تمام ایده‌آلهای اول [اولیه] است (ر.ک. قضیهٔ ۳.۲ (سه)) .

(دو) هر حلقهٔ اول نیمه اول است ، زیرا 0 یک ایده‌آل اول است . این نظیر آن است که هر حلقهٔ اول نیمه ساده است (قضیهٔ ۱۰.۲ (یک)) .

حکم ۳.۴ . *K یک ایده‌آل اول حلقهٔ R است اگر وفقط اگر R/K یک حلقهٔ اول باشد .*

تبصره. این مشابه تعریف ۱۰۲ است (ایده‌آلهای اولیهٔ چپ).

طرح برهان ۳۰۴. اگر R/K اول باشد، $\pi : R \to R/K$ را برورپختی کانونی می‌گیریم. هرگاه I و J ایده‌آلهایی از R باشند به‌طوری که $IJ \subset K$، آنگاه $\pi(I), \pi(J)$ ایده‌آلهایی از R/K اند (تمرین III ۱۳۰۲۰ (ب)) به‌طوری‌که $\pi(I)\pi(J) = \pi(IJ) = 0$. چون R/K اول است، یا $\pi(I) = 0$ یا $\pi(J) = 0$؛ یعنی، $I \subset K$ یا $J \subset K$. بنابراین، K یک ایده‌آل اول می‌باشد (تعریف III ۱۴۰۲۰). عکس مطلب نتیجهٔ ساده‌ای از قضیهٔ III ۱۳۰۲۰ و تعریف III ۱۴۰۲۰ است.

قسمت آخر تشابه نیمه اول ــ نیمه ساده ذیلا" داده شده است.

حکم ۴۰۴. حلقهٔ R نیمه اول است اگر و فقط اگر R با حاصل‌ضرب زیرمستقیمی از حلقه‌های اول یکریخت باشد.

طرح برهان. حکم ۴۰۴ (همان حکم ۲۰۳ است که در آن کلمات "نیمه ساده" و "اولیه" به ترتیب با "نیمه اول" و "اول" عوض شده‌اند. با این تغییر و استفاده از حکم ۳۰۴ به جای تعریف ۱۰۲، می‌توان برهان حکم ۲۰۳ را در حالت فعلی به کار برد.

دیدیم که حلقه‌های اولیه مصالح ساختمانی حلقه‌های نیمه‌ساده‌اند. حکم ۴۰۴ نشان می‌دهد که مصالح ساختمانی حلقه‌های نیمه اول حلقه‌های اول می‌باشند. در اینجا تشابه بین حلقه‌های اولیه و اول فرو می‌ریزد. حلقه‌های اولیه را می‌توان برحسب حلقه‌های ماتریسی آشنا و حلقه‌های درونریختی فضاهای برداری توصیف کرد (بخش ۱). برای حلقه‌های اول نتایج قابل مقایسه وجود ندارند. ولی وضع کاملا" اسف‌بار نیست. ما نتایج بسیار جالبی برای حلقه‌های اولیه و آرتینی چپ نیمه ساده به دست آورده‌ایم (بخشهای ۱ و ۳). درنتیجه، به نظر معقول است که می‌توان توصیفهای مفیدی از حلقه‌های اول و نیمه اول به‌دست آورد که در شرایط زنجیری خاصی صدق کنند، و این دقیقا" کاری است که اینک بدان می‌پردازیم.

ابتدا ملاحظه می‌کنیم که در یک حلقهٔ آرتینی چپ، رادیکال اول با رادیکال

ژاکوبسون یکی است (تمرین ۳ (پ)) . درنتیجه ، حلقه‌های نیمه اول آرتینی چپ نیمه ساده‌نیزهستند ؛ و درنتیجه ، ساختار آنها به وسیلهٔ قضیهٔ ودربورن ــ آرتین ۳۰۳ معین می‌شود . چون هرحلقهٔ آرتینی چپ‌نیمه **اول** (نیمه ساده) بنابر نتیجهٔ ۴۰۳ نوتری چپ نیزهست ، شیءکه‌باید به آن بپردازیم ردهٔ حلقه‌های نوتری چپ نیمه اول است (یعنی ، حلقه‌های نیمه‌اولی که در شرط زنجیر افزایشی بر ایده‌آلهای چپ صدق می‌کنند) . توجه کنیدکه‌حلقه‌های نوتری‌چپ نیمه‌اولی‌وجود دارند که آرتینی چپ نیستند (مثلا " ، $\mathbf{Z}$) . درنتیجه ، توصیف حلقه‌های نوتری چپ نیمه اول تعمیم راستین نتایج قبلی ما می‌باشد .

ما درواقع ردهٔ وسیعتری از حلقه‌ها را توصیف می‌کنیم که حقیقتا " شامل ردهٔ تمام حلقه‌های نوتری چپ نیمه اول است . ردهٔ مورد بحث ردهٔ تمام حلقه‌های گولدی چپ نیمه اول است که‌اینک‌تعریف می‌شود .

خانوادهٔ $\{I_j \mid j \in J\}$ از ایده‌آلهای چپ R را **مستقل** گوییم مشروط بر اینکه به‌ازای هر $k \in J$ ، $I_k \cap I_k^* = 0$ ، که‌درآن I_k^* ایده‌آل‌چپ تولید شده به وسیلهٔ $\{I_j \mid j \neq k\}$ است . به عبارت دیگر ، $\{I_j \mid j \in J\}$ مستقل است اگر و فقط اگر ایده‌آل چپ I تولید شده به وسیلهٔ $\{I_j \mid j \in J\}$ مجموع مستقیم داخلی $I = \sum_{j \in J} I_j$ باشد (ر.ک. قضیهٔ IV ۱۵۰۱۰) .

تعریف ۵۰۴ . حلقهٔ R را یک **حلقهٔ گولدی** *(چپ)* گوییم اگر
(یک) R در شرط زنجیر افزایشی بر صفرسازهای چپ صدق کند ؛
(دو) هر مجموعهٔ مستقل از ایده‌آلهای چپ R متناهی باشد .

چند تبصره . (یک) شرط (یک) تعریف ۵۰۴ یعنی به‌ازای هر زنجیر از صفرسازهای چپ مانند $\mathcal{A}(S_1) \subset \mathcal{A}(S_2) \subset \cdots$ ، n ی وجود دارد به‌طوری که به‌ازای هر $i \geq n$ ، $\mathcal{A}(S_i) = \mathcal{A}(S_n)$. این شرط با شرط زیر معادل است .
(یک′) R در شرط ماکزیمم بر صفرسازهای چپ صدق می‌کند (یعنی ، هر مجموعهٔ ناتهی از صفرسازهای چپ نسبت به شمول نظریهٔ مجموعه‌ها عنصر ماکزیمال دارد) .

برای اثبات این امر کافی است ملاحظه شود که برهان قضیهٔ VIII ۴۰۱۰ در وضع فعلی **نعل به نعل** قابل بیان است .

(دو) حلقه‌های گولدی راست به نحو روشنی تعریف می‌شوند . یک حلقهٔ گولدی راست

لزوما " حلقهٔ گولدی چپ نیست؛ ر.ک. ا. دبلیو. گولدی [۶۲].

مثال. هرحلقهٔ نوتری چپ R یک‌حلقهٔ گولدی چپ است. شرط (یک) بوضوح برقرار است. هرگاه $\{I_j \mid j \in J\}$ یک مجموعهٔ مستقل نامتناهی از ایده‌آلهای چپ می‌بود، آنگاه $I_1, I_2, \ldots$ وجود داشتند به‌طوری که $I_1 \subsetneq I_1 \times I_2 \subsetneq I_1 \times I_2 \times I_3 \subsetneq \cdots$، که شرط زنجیر افزایشی را نقض می‌کرد. بنابراین، شرط (دو) برقراراست و R یک حلقهٔ گولدی می‌باشد. حلقه‌های گولدی چپی وجود دارند که حلقه‌های نوتری چپ **نیستند**.

مثال فوق نشان‌می‌دهدکه‌ردهٔ حلقه‌های گولدی چپ نیمه اول شامل ردهٔ حلقه‌های نوتری‌چپ‌نیمه اول است. توصیف ما از حلقه‌های گولدی چپ نیمه اول برحسب حلقه‌های خارج‌قسمتی چپ آنها، و در قالب تعاریف زیر، داده خواهد شد.

تعریف ۶.۴. گوییم عنصرناصفر a در حلقهٔ R ***منتظم*** است اگر $\bar{a}$ نه مقسوم‌علیه صفر چپ باشد نه مقسوم‌علیه صفر راست.

تعریف ۷.۴. حلقهٔ یکدار $Q(R)$ را یک ***حلقهٔ خارج‌قسمتی چپ*** حلقهٔ R نامیم اگر
(یک) $R \subset Q(R)$؛
(دو) هر عنصر منتظم در R یک یکه در $Q(R)$ باشد؛
(سه) هر عنصر c از $Q(R)$ به شکل $c = a^{-1}b$ باشد، که در آن $a,b \in R$ و a منتظم می‌باشد.

چند تبصره. (یک) لازم نیست حلقهٔ R حلقهٔ خارج‌قسمتی چپ داشته باشد. اما، درصورت‌داشتن، طبق‌تعریف ۷.۴، به‌آسانی معلوم می‌شود که $Q(R)$ با تقریب یکریختی معین است.
(دو) یک حلقهٔ خارج‌قسمتی راست R به همین نحو تعریف می‌شود، جز آنکه در شرط (سه) باید "$c = a^{-1}b$" را با "$c = ba^{-1}$" عوض‌کرد. یک‌حلقه‌ممکن‌است حلقهٔ خارج‌قسمتی

راست داشته‌باشد ولی حلقهٔ خارج‌قسمتی چپ نداشته باشد (ر.ک. ان. ج. دیوینسکی [۲۲؛ ص ۷۱]).

(سه) هرگاه حلقهٔ R دارای حلقهٔ خارج‌قسمتی چپ $Q(R) = T$ باشد، آنگاه گوییم R یک **ترتیب چپ** در T است.

مثال. فرض کنیم R حلقهٔ تعویضپذیری باشد که دست‌کم یک عنصر منتظم دارد. همچنین، S مجموعهٔ تمام عناصر منتظم R باشد. در این صورت، حلقهٔ تام خارج‌قسمتهای $S^{-1}R$ حلقه‌ای یکدار است (قضیهٔ III ۳.۴۰) که شامل یک نسخهٔ یکریخت $\varphi_S(R)$ از R می‌باشد (قضیهٔ III ۴.۴۰ (دو)). هرگاه طبق معمول R و $\varphi_S(R)$ را یکی کنیم، آنگاه $R \subset S^{-1}R$، هرعنصر منتظم R یک یکه در $S^{-1}R$ است (قضیهٔ III ۴.۴۰ (یک)) و هر عنصر $S^{-1}R$ به شکل rs^{-1} $(r \in R, s \in S \subset R)$ می‌باشد. بنابر این، $S^{-1}R$ یک حلقهٔ خارج‌قسمتی چپ R است.

حالت خاص: میدان‌گویای $\mathbf{Q}$ یک‌حلقهٔ خارج‌قسمتی چپ حلقهٔ نوتری چپ $\mathbf{Z}$ می‌باشد.

مثال. هر حلقهٔ آرتینی چپ نیمه ساده حلقهٔ خارج قسمتی چپ خود می‌باشد (تمرین ۶).

از تعریف ۷.۴ واضح است که ساختار حلقهٔ خارج‌قسمتی چپ $Q(R)$ با ساختار حلقهٔ R رابطهٔ نزدیک دارد. درنتیجه، اگر بتوان حلقهٔ R را برحسب حلقه‌های شناخته شده به‌طور صریح توصیف کرد، بهترین کار این است که نشان دهیم R دارای یک حلقهٔ خارج‌قسمتی چپ است که برحسب این حلقه‌ها به‌طور صریح قابل بیان است. این دقیقاً کاری است که قضیهٔ گولدی برای ما می‌کند.

قضیهٔ ۸.۴ (گولدی) *R یک حلقهٔ گولدی چپ [اول] نیمه اول است اگر و فقط اگر R دارای یک حلقهٔ خارج‌قسمتی چپ چون Q(R) باشد که آرتینی چپ [ساده] نیمه‌ساده است.*

قضیهٔ ۸.۴ را به خاطر ضیق جا ثابت نمی‌کنیم. یکی از بهترین برهانها از آن سی. پروسسی[1] و ال. اسمال[2] [۶۵] است؛ صورت کمی تعمیم یافته‌ای از آن را در آی. هراشتاین [۲۴] می‌بینیم. این برهان، با آنکه طولانی است، از بسیاری از برهانهایی که قبلا" در این فصل آمده‌اند مشکلتر نیست. در آن از قضیهٔ اور[3] استفاده شده است، که برهانش به اختصار در آی. ان. هراشتاین [۲۴ ؛ ص ۱۷۰] و به تفصیل در ان. ج. دیوینسکی [۲۲ ؛ ص ۶۶] آمده است.

چون ساختار حلقه‌های آرتینی چپ نیمه ساده کاملا" معین شده است، قضیهٔ ۸.۴ چنان توصیف مناسبی به دست می‌دهد که شاید حلقه‌های گولدی چپ نیمه اول (حالت خاص: حلقه‌های نوتری چپ نیمه اول) به دست آیند. "فاصلهٔ" بین حلقه‌های R و $Q(R)$ تاوانی است که باید برای تعویض شرط زنجیرکاهشی با شرط زنجیرافزایشی پرداخت. زیرا، همانطور که در بحث بعد از حکم ۴.۴ و تمرین ۱۳.۳ دیدیم، شرط دوم از شرط اول بسیار ضعیفتر است.

نتیجهٔ ۹.۴. *R یک حلقهٔ گولدی چپ [اول] نیمه اول است اگر و فقط اگر R یک حلقهٔ خارج‌قسمتی مانند $Q(R)$ داشته باشد به طوری که* $Q(R) \cong Mat_{n_1}D_1 \times \cdots \times Mat_{n_k}D_k$ [$Q(R) \cong Mat_{n_1}D_1$]، *که در آن $n_1, \ldots, n_k$ اعداد صحیح مثبتی بوده و $D_1, \ldots, D_n$ حلقه‌هایی بخشی می‌باشند.*

برهان. قضایای ۱۴.۱، ۳.۳، و ۸.۴.

قضیهٔ گولدی، به صورت نتیجهٔ ۹.۴، را می‌توان تعمیمی از قضایای ودربورن ـ آرتین ۱۴.۱ و ۳.۳ به ردهٔ وسیعتر حلقه‌ها درنظر گرفت. مثلا"، قضیهٔ ۳.۳ می‌گوید که یک حلقهٔ آرتینی چپ نیمه ساده حاصلضرب مستقیمی از حلقه‌های ماتریسی روی حلقه‌های بخشی است. قضیهٔ گولدی می‌گوید که هر حلقهٔ گولدی چپ نیمه اول دارای یک حلقهٔ خارج‌قسمتی است که حاصلضرب مستقیمی از حلقه‌های ماتریسی روی حلقه‌های بخشی می‌باشد. اما هر حلقهٔ آرتینی چپ نیمه ساده یک حلقهٔ گولدی چپ نیمه اول است

---

1. C. Procesi
2. L. Small
3. Ore

(نتیجهٔ ۴.۳، تمرین ۳ (آ)، ومثال بعد از تعریف ۵.۴). به علاوه، هر حلقهٔ آرتینی چپ نیمه ساده حلقهٔ خارج‌قسمتی خود می‌باشد (تمرین ۶). لذا، در این حالت قضیهٔ گولدی به قضیهٔ ودربورن ــ آرتین تحویل می‌شود. استدلالی مشابه برای حلقه‌های آرتینی چپ ساده و قضیهٔ ۱۴.۱ برقرار است.

تمرینات

تذکر. R همواره یک حلقه است.

۱. زیرمجموعهٔ T از R را یک **m ــ دستگاه** (دستگاه ضربی تعمیم یافته) گویند اگر به‌ازای $x \in R$، $c,d \in T \Rightarrow cxd \in T$.

(آ) P یک ایده‌آل اول R است اگر و فقط اگر $R - P$ یک m ــ دستگاه باشد. [**راهنمایی.** تمرین III ۱۴.۲۰].

(ب) فرض کنید I ایده‌آلی از R باشد که از m ــ دستگاه T جدا می‌باشد. نشان دهید که I مشمول ایده‌آلی چون Q است که نسبت به خاصیت $Q \cap T = \varnothing$ ماکزیمال است. سپس نشان دهید که Q یک ایده‌آل اول است. [**راهنمایی.** از برهان قضیهٔ VIII ۲.۲۰ تقلید کنید.]

(پ) گوییم عنصر r از R دارای **خاصیت صفر** است اگر هر m ــ دستگاهی که شامل r باشد شامل 0 نیز باشد. نشان دهید که رادیکال اول $P(R)$ مجموعهٔ M مرکب ازتمام عناصر R است که دارای خاصیت صفر می‌باشند. [**راهنمایی.** بااستفاده از (آ)، نشان دهید که $M \subset P(R)$ و، بااستفاده از (ب)، نشان دهید $P(R) \subset M$.]

(ت) هر عنصر c از $P(R)$ پوچ‌توان است. [**راهنمایی.** $\{c^i \mid i \geq 1\}$ یک m ــ دستگاه است. اگر R تعویضپذیر باشد، $P(R)$ از تمام عناصر پوچ‌توان R تشکیل شده است.]

۲. (آ) هرگاه I ایده‌آلی از R باشد، آنگاه $P(I) = I \cap P(R)$. بخصوص، $P(P(R)) = P(R)$. [**راهنمایی.** تمرین ۱ (پ).]

(ب) $P(R)$ کوچکترین ایده‌آل K از R است که $P(R/K) = 0$. بخصوص، $P(R/P(R)) = 0$، که از آنجا $R/P(R)$ نیمه اول است. [**راهنمایی.** تمرین III ۱۷.۲۰ (ت).]

(پ) گوییم ایده‌آل I دارای **خاصیت صفر** است اگر هر عنصر I خاصیت صفر

داشته باشد (تمرین ۱ (پ)).

نشان دهید که خاصیت صفر یک خاصیت رادیکال (به‌صورت تعریف شده در مقدمهٔ بخش ۲) است که رادیکال آن دقیقاً "$P(R)$" می‌باشد.

۳. (آ) هر حلقهٔ نیمه ساده نیمه اول است.

(ب) $P(R) \subset J(R)$. [**راهنمایی.** تمرین ۱ (ت)؛ یا (آ) و تمرین ۲ (ب).]

(پ) اگر R آرتینی چپ باشد، $P(R) = J(R)$. [**راهنمایی.** حکم ۱۳.۲.]

۴. R نیمه اول است اگر و فقط اگر به‌ازای جمیع ایده‌آلهای A, B

$$AB = 0 \Rightarrow A \cap B = 0.$$

۵. (آ) فرض کنید R حلقه‌ای یکدار باشد. حلقهٔ ماتریسی $\mathrm{Mat}_n R$ اول است اگر و فقط اگر R اول باشد.

(ب) هرگاه R حلقه باشد، آنگاه $P(\mathrm{Mat}_n R) = \mathrm{Mat}_n P(R)$. [**راهنمایی.** اگر R یکدار باشد، از تمرین ۲ و قسمت (آ) استفاده کنید. در حالت کلی، R را طبق قضیهٔ III ۱۰.۱۰ در حلقهٔ S بنشانید؛ در این صورت، طبق تمرین ۲، $P(R) = R \cap P(S)$.]

۶. هرگاه R آرتینی چپ نیمه ساده باشد، آنگاه R حلقهٔ خارج‌قسمتی خود می‌باشد. [**راهنمایی.** چون R طبق قضیهٔ ۳.۳ یکدار است، کافی است نشان دهیم که هر عنصر منتظم R درواقع یکه است. بنابر قضیهٔ ۳.۳ و استدلالی مستقیم، کافی است فرض شود که به‌ازای حلقه‌ای بخشی مانند D، $R = \mathrm{Mat}_n D$. قضیهٔ VII ۶.۲۰ و حکم VII ۱۲.۲۰ ممکن است مفید باشند.]

۷. احکام زیر باهم معادلند:

(آ) R اول است؛

(ب) $a, b \in R$ و $aRb = 0$ ایجاب می‌کنند که $a = 0$ یا $b = 0$؛

(پ) صفرساز راست هر ایده‌آل راست ناصفر R مساوی 0 است؛

(ت) صفرساز چپ هر ایده‌آل چپ ناصفر R مساوی 0 است.

۸. هر حلقهٔ اولیه اول است [ر.ک. تمرین ۷].

۹. مرکز هر حلقهٔ اول یکدار یک دامنهٔ صحیح است. [ر.ک. تمرین ۷؛ برای عکس مطلب، ر.ک. تمرین ۱۰.]

۱۰. فرض کنید J دامنهٔ صحیحی بوده و F میدان تام خارج‌قسمتهای J باشد. همچنین،

R مجموعهٔ تمام ماتریسهای نامتناهی (سطرها و ستونها با $\mathbf{N}^*$ اندیسگذاری شده‌اند) به شکل زیر باشد:

$$\begin{pmatrix} A_n & & & & 0 \\ & d & & & \\ & & d & & \\ & & & d & \\ & & & & \ddots \\ 0 & & & & \ddots \end{pmatrix}$$

که در آن $A_n \in \mathrm{Mat}_n(F)$ و $d \in J \subset F$.

(آ) R یک حلقه است.

(ب) مرکز R مجموعهٔ تمام ماتریسها به شکل

$$\begin{pmatrix} d & & & & 0 \\ & d & & & \\ & & d & & \\ & & & \ddots & \\ 0 & & & & \ddots \end{pmatrix}$$

است که $d \in J$ ؛ و درنتیجه، با J یکریخت است.

(پ) R اولیه است (و درنتیجه، بنابر تمرین ۸، اول می‌باشد).

۱۱. **هیچ رادیکال** $N(R)$ از R ایده‌آل تولید شده به وسیلهٔ مجموعهٔ تمام ایده‌آلهای پوچ R است.

(آ) $N(R)$ یک ایده‌آل پوچ است.

(ب) $N(N(R)) = N(R)$.

(پ) $N(R/N(R)) = 0$.

(ت) $P(R) \subset N(R) \subset J(R)$.

(ث) اگر R آرتینی چپ باشد، $P(R) = N(R) = J(R)$.

(ج) اگر R تعویضپذیر باشد، $P(R) = N(R)$.

۵ جبرها

مفاهیم و نتایج بخشهای ۱ تا ۳ به جبرها روی حلقهٔ تعویضپذیر و یکدار K سرایت می‌کنند.

بخصوص، قضیهٔ ودربورن ــ آرتین برای K ــ جبرها ثابت شده است (قضیهٔ ۴۰۵) . در قسمت دوم بخش به جبرهای روی یک میدان ، به انضمام جبرهای جبری و جبر گروهی یک گروه متناهی ، می‌پردازیم . در سراسر این بخش، K ***همواره یک حلقهٔ تعویضپذیر یکدار است .***

اولین گام در بیان نتایج بخشهای ۱ تا ۳ به K ــ جبرها مرور تعاریف K ــ جبر ، همریختی K ــ جبرها ، یک زیرجبر و یک ایده‌آل جبر است (بخش IV ۷۰) . به یاد می‌آوریم که ***هرگاه K ــ جبر A یکدار باشد ، آنگاه ایده‌آلهای جبر (چپ ، راست ، دوطرفه) با ایده‌آلهای (چپ ، راست ، دوطرفه) حلقهٔ A یکی است .*** (ر.ک. تبصره‌های بعد از تعریف IV ۳۰۷۰) . از این امر بارها بدون ذکر صریح استفاده خواهد شد .

K ــ جبر آرتینی چپ K ــ جبری است که در شرط زنجیری کاهشی بر ایده‌آلهای چپ جبر صدق می‌کند . یک K ــ جبر آرتینی چپ ممکن است یک حلقهٔ آرتینی چپ نباشد (تمرین ۱) .

مثال . هرگاه D یک جبر بخشی روی K باشد ، آنگاه $\mathrm{Mat}_n D$ ، K ــ جبری است (ص ۳۵۶) که طبق نتیجهٔ VIII ۱۲۰۱۰ آرتینی چپ است .

تعریف ۱.۵. فرض کنیم A یک جبر روی حلقهٔ تعویضپذیر و یکدار K باشد .

(یک) یک ***(جبر) A ــ مدول چپ*** یک K ــ مدول چپ یکانی مانند M است به‌طوری که M روی حلقهٔ A مدول چپ بوده و به‌ازای هر $k \in K, r \in A, c \in M$ ، $k(rc) = (kr)c = r(kc)$.

(دو) A ــ زیرمدول A ــ مدول M زیرمجموعه‌ای از M است که خود یک جبر A ــ مدول (تحت اعمال در M) می‌باشد .

(سه) جبر A ــ مدول M ***ساده*** (یا ***تحویل‌ناپذیر***) است اگر $AM \neq 0$ و M هیچ A ــ زیرمدول حقیقی نداشته باشد .

(چهار) ***همریختی*** $f : M \to N$ از جبر A ــ مدولها نگاشتی است که هم یک K ــ مدول و هم همریختی A ــ مدولها می‌باشد .

چند تبصره . اگر A یک K ــ جبر باشد ، اصطلاح " A ــ مدول " همواره به معنی جبر

A ــ مدول است. مدولهای روی **حلقهٔ** A به این طریق نامگذاری می‌شوند. A ــ مدول راست N به‌همین‌نحوتعریف‌شده‌و در $k(cr) = (kc)r = c(kr)$ به‌ازای هر $k \in K, r \in A, c \in N$ صدق می‌کند.

حال K ــ جبرهای ساده، K ــ جبرهای اولیه، رادیکال ژاکوبسون یک K ــ جبر، K ــ جبرهای نیمه ساده، و غیره همانند مفاهیم نظیر برای حلقه‌ها تعریف می‌شوند؛ همچنین، ایده‌آلهای جبر، مدولها، همریختیها، و غیره به جای ایده‌آلهای حلقه، مدولها، وهمریختیهاتعریف می‌گردند. برای بیان نتایج بخشهای ۱ تا ۳ به K ــ جبرها (بخصوص، قضایای ودربورن ــ آرتین)، دو قضیهٔ زیر مفید خواهند بود.

قضیهٔ ۲۰۵. *فرض کنیم A یک K ــ جبر باشد.*
(یک) *زیرمجموعهٔ I از A یک ایده‌آل جبر چپ ماکزیمال منتظم است اگر و فقط اگر I یک ایده‌آل چپ ماکزیمال منتظم حلقهٔ A باشد.*
(دو) *رادیکال ژاکوبسون حلقهٔ A با رادیکال ژاکوبسون جبر A یکی است. بخصوص، A یک حلقهٔ نیمه ساده است اگر و فقط اگر A یک جبر نیمه ساده باشد.*

تبصره. قضیهٔ ۲۰۵ در صورتی که A یکدار باشد بدیهی است، زیرا ایده‌آلهای جبر و ایده‌آلهای حلقه در این حالت یکی هستند.

برهان ۲۰۵. (یک) اگر I یک ایده‌آل چپ ماکزیمال منتظم حلقهٔ A باشد، کافی است‌نشان‌دهیم که به‌ازای هر $k \in K$، $kI \subset I$. فرض‌کنیم به‌ازای $k \in K$ ای، $kI \not\subset I$. چون‌طبق‌تعریف ۱۰۵ (یک) $r(kI) = k(rI)$، $I + kI$ یک ایده‌آل‌چپ A است که حقیقتاً شامل I می‌باشد. بنابراین، طبق ماکزیمالی، $A = I + kI$. بنابه فرض، $e \in A$ ای وجوددارد‌به‌طوری‌که‌به‌ازای هر $r \in A$، $r - re \in I$. فرض‌کنیم $e = a + kb$ $(a,b \in I)$. در این صورت،

$$e^2 = e(a + kb) = ea + e(kb) = ea + (ke)b \in I.$$

چون $e - e^2 \in I$ و $e^2 \in I$، باید داشته باشیم $e \in I$. درنتیجه، این امر که به‌ازای هر $r \in A$، $r - re \in I$، ایجاب می‌کند که $A = I$، و این با ماکزیمالی I در تضاد است.

بنابراین، به‌ازای هر $k \in K$، $kI \subset I$.

به عکس، فرض کنیم I یک ایده‌آل جبر چپ ماکزیمال منتظم بوده؛ و درنتیجه، یک ایده‌آل چپ منتظم حلقهٔ A باشد. بنابر لم ۴.۲، I مشمول یک ایده‌آل چپ ماکزیمال منتظم مانند I_1 از حلقهٔ A است. بند پیشین نشان می‌دهد که I_1 درواقع یک ایده‌آل جبر چپ منتظم است؛ درنتیجه، طبق ماکزیمالی، $I = I_1$.

قسمت (دو) از قسمت (یک) و قضیهٔ ۳.۲ (دو) نتیجه می‌شود.

قضیهٔ ۳.۵. *فرض کنیم A یک K ــ جبر باشد. هر جبر A ــ مدول ساده یک مدول ساده‌روی‌حلقهٔ A است. به‌هر مدول سادهٔ M روی حلقهٔ A می‌توان ساختار K ــ مدول منحصر به فرد داد به نحوی که M یک جبر A ــ مدول ساده باشد.*

برهان. فرض کنیم N یک جبر A ــ مدول‌ساده باشد؛ درنتیجه، $AN \neq 0$. هرگاه N_1 یک زیرمدول N باشد، آنگاه AN_1 یک جبر زیرمدول N است، که از آنجا $AN_1 = N$ یا $AN_1 = 0$. هرگاه $AN_1 = N$، آنگاه $N_1 = N$. هرگاه $AN_1 = 0$، آنگاه

$$N_1 \subset D = \{c \in N \mid Ac = 0\}.$$

اما D یک جبر زیرمدول N است و $D \neq N$، زیرا $AN \neq 0$. بنابراین، طبق سادگی، $D = 0$، که از آنجا $N_1 = 0$. درنتیجه، N زیرمدول حقیقی ندارد؛ و لذا، یک مدول ساده روی حلقهٔ A است.

هرگاه M یک مدول ساده روی حلقهٔ A باشد، آنگاه، بنابر تبصرهٔ (سه) بعد از تعریف ۱.۱، M دوری‌است؛ مثلاً "، $M = Ac\ (c \in M)$. ساختار K ــ مدول‌بر $M = Ac$ را با

$$k(rc) = (kr)c, \quad (k \in K, r \in A)$$

تعریف می‌کنیم. چون $kr \in A$، $(kr)c$ عنصری از $Ac = M$ است. برای آنکه نشان دهیم عمل K بر M تعریف شده است، باید نشان دهیم که

$$rc = r_1c \ \Rightarrow\ (kr)c = (kr_1)c, \quad (k \in K;\ r, r_1 \in A).$$

واضح است که باید ثابت کنیم

$$rc = 0 \ \Rightarrow\ (kr)c = 0, \quad (k \in K, r \in A).$$

اما، طبق قضیهٔ ۳.۱، $M \cong A/I$، که در آن ایده‌آل چپ ماکزیمال منتظم I هستهٔ

نگاشت $A \to Ac = M$ داده شده با $x \mapsto xc$ است. درنتیجه، $rc = 0$ ایجاب می‌کند که $r \in I$. اما I طبق قضیهٔ ۴۰۵ یک ایده‌آل جبر است؛ که از آنجا $kr \in I$. بنابراین، $(kr)c = 0$ و عمل K بر M تعریف شده است. حال به آسانی تحقیق می‌شود که M یک K ــ مدول و یک جبر A ــ مدول است. ساختار K ــ مدول M منحصر به فرد است، زیرا هر ساختار K ــ مدول بر M که $M = Ac$ رایک A ــ مدول‌سازد لزوماً در $k(rc) = (kr)c$ به‌ازای هر $k \in K, r \in A$ صدق می‌کند.

قضیهٔ ۴۰۵. *A یک K ــ جبر آرتینی چپ نیمه ساده است اگر و فقط اگر یک یکریختی از K ــ جبرها مانند*

$$A \cong Mat_{n_1}D_1 \times Mat_{n_2}D_2 \times \cdots \times Mat_{n_t}D_t$$

موجود باشد، که در آن هر n_i عدد صحیح مثبتی بوده و هر D_i یک جبر بخشی روی K است.

تبصره. قضیهٔ ۴۰۵ برای هر جبر با بعد متناهی نیمه سادهٔ A روی میدان K برقرار است، زیرا یک چنین A آرتینی چپ می‌باشد (تمرین ۲).

طرح برهان ۴۰۵. با استفاده ازقضایای ۲۰۵ و ۳۰۵ و تمرینهای ۳ و ۴، برهان قضیهٔ ودربورن ــ آرتین ۳۰۳ را در مورد K ــ جبرها به کار برید.

تاپایان این بخش به چند مطلب خاص در باب جبرها روی یک میدان می‌پردازیم. ابتدا صورت قویتری از قضیهٔ ۴۰۵ را درحالتی به دست می‌آوریم که K یک میدان به‌طور جبری بسته باشد و بالاخره جبرهای گروه روی یک میدان را درنظر خواهیم گرفت.

هرگاه A یک جبر ناصفر یکدار روی میدان K باشد، آنگاه به آسانی معلوم می‌شود که نگاشت $\alpha : K \to A$، تعریف شده با $k \mapsto k1_A$، یک همریختی K ــ جبرهاست. چون $\alpha(1_K) = 1_A \neq 0$، داریم $\ker \alpha \neq K$. اما میدان K ایده‌آل حقیقی ندارد، که از آنجا $\operatorname{Ker} \alpha = 0$. لذا، α یک تکریختی است. به علاوه، نقش α در مرکز A است، زیرا به‌ازای هر $k \in K, r \in A$،

$$\alpha(k)r = (k1_A)r = k(1_Ar)1_A = (1_Ar)(k1_A) = r\alpha(k).$$

درنتیجه، قرارداد زیر را می‌پذیریم.

هرگاه A یک جبر ناصفر یکدار روی میدان K باشد، آنگاه K با $Im\,\alpha$ یکی شده و زیر جبری از مرکز A درنظر گرفته می‌شود.

تحت این انطباق، عمل K ــ مدول K بر A با ضرب در عناصر زیرجبرهای K در A یکی می‌شود، زیرا $ka = (k1_A)a = \alpha(k)a$.

تعریف ۵۰۵. عنصر a از جبر A روی میدان K را **جبری** روی K نامیم اگر a ریشه‌ای از یک چندجمله‌ای در K[x] باشد. گوییم A یک **جبر جبری** روی K است اگر هر عنصر A روی K جبری باشد.

مثال. هرگاه A با بعد متناهی باشد، آنگاه A یک جبر جبری است. زیرا هرگاه $\dim_K A = n$ و $a \in A$، آنگاه $n+1$ عنصر $a, a^2, a^3, \ldots, a^{n+1}$ باید وابستهٔ خطی باشند. لذا، به‌ازای $k_i \in K$ هایی که همه‌صفر نیستند، $k_1a + k_2a^2 + \cdots + k_{n+1}a^{n+1} = 0$. لذا، $f(a) = 0$، که در آن f چندجمله‌ای ناصفر $k_1x + k_2x^2 + \cdots + k_{n+1}x^{n+1} \in K[x]$ می‌باشد.

مثال. جبر ماتریسهای شمارشپذیر نامتناهی روی میدان K که فقط تعدادی متناهی از درایه‌هایشان ناصفرند یک جبر جبری ساده با بعد نامتناهی است (تمرین ۵).

تبصره. رادیکال یک جبر جبری پوچ است (تمرین ۶).

لم ۶۰۵. هرگاه D یک جبربخشی جبری‌روی‌میدان به‌طور جبری بستهٔ K باشد، آنگاه $D = K$.

برهان. بنابر قرارداد فوق، K مشمول مرکز D است. هرگاه $a \in D$، آنگاه به‌ازای $f \in K[x]$ی، $f(a) = 0$. چون K به‌طور جبری بسته است،

$$f(x) = k(x - k_1)(x - k_2)\cdots(x - k_n)\ (k, k_i \in K;\ k \neq 0),$$

که از آنجا

$$0 = f(a) = k(a - k_1)(a - k_2)\cdots(a - k_n).$$

چون D حلقهٔ بخشی است، به‌ازای iی $a - k_i = 0$. بنابراین، $a = k_i \in K$؛ و لذا،

$D \subset K$.

قضیهٔ ۷۰۵ . *فرض کنیم A یک جبر نیمه ساده با بعد متناهی روی میدان به‌طور جبری بستهٔ K باشد . در این صورت ، اعداد صحیح مثبتی مانند* $n_1, \ldots, n_t$ *و یک یکریختی از K ــ جبرها چون*

$$A \cong Mat_{n_1}K \times \cdots \times Mat_{n_t}K$$

وجود خواهند داشت .

برهان . بنابر قضیهٔ ۴۰۵ (و تبصرهٔ بعد از آن) ،

$$A \cong \mathrm{Mat}_{n_1}D_1 \times \mathrm{Mat}_{n_2}D_2 \times \cdots \times \mathrm{Mat}_{n_t}D_t$$

که در آن هر D_i یک جبربخشی روی K است . هر D_i لزوما " روی K با بعد متناهی است (در غیر این صورت ، $\mathrm{Mat}_{n_i}D_i$ و درنتیجه A با بعدنامتناهی می‌باشد) . بنابراین ، طبق لم ۶۰۵ ، به‌ازای هر i ، $D_i = K$.

سالهاست که تحقیقات زیادی در جبرهای گروهی‌روی یک میدان می‌شود(ر .ک . ص ۳۵۵) . ایــن جبرها مفیدند ، زیرا به کمک آنها می‌توان از تکنیکهای نظریهٔ حلقه‌ها در بررسی گروهها استفاده کرد .

حکم ۸۰۵ . *(مشکه[1]) فرض کنیم K(G) یک جبرگروهی از گروه متناهی G روی میدان K باشد . هــرگاه K دارای مشخــص 0 باشد ، آنگاه K(G) نیمه‌ساده‌است . هرگاه K دارای مشخص اول p باشد ، آنگاه K(G) نیمه ساده است اگر و فقط‌اگر p ، |G| را عاد نکند .*

طرح برهان . فرض کنیم $\mathrm{char}\ K$ مساوی 0 یا p باشد ،که $p \nmid |G|$. اگر B یک K ــ جبر یکدار (بخصوص $K(G)$) باشد ، تحقیق کنیــد یک تکریختی تعریف شده از K ــ جبرها مانند $\alpha : B \to \mathrm{Hom}_K(B,B)$ به صورت زیــر وجود دارد : $\alpha(b)$ مساوی نگاشت $\alpha_b : B \to B$ است ، که در آن $\alpha_b(x) = bx$.

---

1. *Maschke*

اگر $g \in G$ ، عنصر $1_K g$ از $K(G)$ را با g نشان می‌دهیم . بنابر تعریف ، $K(G)$ یک K ــ فضای برداری با پایهٔ $X = \{g \mid g \in G\}$ و بعد متناهی $n = |G|$ است . به‌ازای هر $u \in K(G)$ ، M_u راماتریس α_u نسبت‌به پایهٔ X می‌گیریم . فرض کنیم $g \in G$ که $g \neq e$. در این صورت ، به‌ازای هر $g_1 \in G$ ، $\alpha_g(g_1) = gg_1 \neq g_1$ (زیرا G گروه است) . لذا ، α_g صرفا "عناصرپایهٔ X را باهم تعویض کرده و هیچ‌عنصرپایه را ثابت نمی‌گذارد . درنتیجه ، ماتریس M_g ی α_g نسبت به پایهٔ X را می‌توان از ماتریس همانی I_n با جایگشت مناسبی از سطرها که هیچ سطری را ثابت نمی‌گذارد به دست آورد (ر.ک. قضیهٔ VII ۲۰۱۰) . به یاد آورید که اثر ، یعنی $\operatorname{Tr} M_u$ ، مجموع درایه‌های قطر اصلی M_u است (ر.ک. ص ۵۷۵) . به آسانی معلوم می‌شود که

(یک) به‌ازای $g \in G, g \neq e$ ، $\operatorname{Tr} M_g = 0$ ؛

(دو) $M_e = I_n$ ، که از آنجا $\operatorname{Tr} M_e = n1_K$ ؛

(سه) هرگاه $u = k_1 g_1 + \cdots + k_n g_n \in K(G)$ ، آنگاه

$$\alpha_u = \sum_{i=1}^{n} k_i \alpha_{g_i} \quad \text{و} \quad \operatorname{Tr} M_u = \sum_{i=1}^{n} k_i \operatorname{Tr} M_{g_i}.$$

هرگاه رادیکال J از $K(G)$ ناصفر باشد ، آنگاه عنصر ناصفری چون $v \in J$ وجود دارد که $v = k_1 g_1 + \cdots + k_n g_n$. می‌توان فرض کرد که $g_1 = e$ و $k_1 = 1_K$ (در غیر این صورت ، v را با $k_i^{-1} g_i^{-1} v$ عوض می‌کنیم که در آن $k_i \neq 0$ ومجددا "شماره‌گذاری می‌نماییم) . چون $K(G)$ بابعدمتناهی‌روی K است ، $K(G)$ آرتینی‌چپ است (تمرین ۲) . درنتیجه ، طبق حکم ۱۳۰۲ (برای جبرها) J پوچ‌توان می‌باشد . بنابراین ، $v \in J$ پوچ توان است که از آنجا α_v پوچ توان می‌باشد . لذا ، طبق قضیهٔ VII ۳۰۱۰ ، M_v یک ماتریس پوچ‌توان می‌باشد . بنابراین ، $\operatorname{Tr} M_v = 0$ (تمرین VII ۱۰۰۵۰) . از آن سو ، قسمتهای (یک) تا (سه) فوق ایجاب می‌کنند که

$$\begin{aligned} \operatorname{Tr} M_v &= \sum_{i=1}^{n} k_i \operatorname{Tr} M_{g_i} = 1_K \operatorname{Tr} M_e + \sum_{i=2}^{n} k_i \operatorname{Tr} M_{g_i} \\ &= \operatorname{Tr} M_e + 0 = n1_K. \end{aligned}$$

اما $n1_K \neq 0$ ، زیرا $\operatorname{char} K = 0$ یا $\operatorname{char} K = p$ و $p \nmid |G| = n$ را عاد نمی‌کند ، و این یک تناقض می‌باشد . بنابراین $J = 0$ و $K(G)$ نیمه ساده است .

به عکس ، فرض کنیم $\operatorname{char} K = p$ و $p \mid n$. همچنین ، w مجموع تمام عناصر پایهٔ X در $K(G)$ باشد ؛ یعنی ، $w = g_1 + g_2 + \cdots + g_n \in K(G)$. واضح است که $w \neq 0$.

تحقیق کنید که به‌ازای هر $g \in G$ ، $wg = gw$ ، که ایجاب می‌کند که w در مرکز $K(G)$ باشد. نشان دهید $w^2 = nw = (n1_K)w$ ، که از آنجا $w^2 = 0$ (زیرا $p \mid n$). لذا ، $(K(G)w)(K(G)w) = 0$ ؛ درنتیجه ،ایده‌آل چپ ناصفر $K(G)w$ پوچ‌توان است. چون بنابر قضیهٔ ۱۲.۲ ، $K(G)w \subset J$ ، پس $J \neq 0$. بنابراین ، $K(G)$ نیمه ساده نیست.

نتیجهٔ زیر (درصورتی که K میدان اعداد مختلط باشد) در مطالعهٔ نمایشها و مشخصه‌های گروههای متناهی کاملا" مفید می‌باشد.

نتیجهٔ ۹.۵ . *فرض کنیم $K(G)$ جبر گروه یک گروه متناهی G روی میدان به‌طور جبری بسته‌ٔ K باشد. هرگاه $char\ K = 0$ یا $char\ K = p$ و $p \nmid |G|$ ، آنگاه اعداد صحیح مثبتی چون $n_1, \ldots, n_t$ و یک یکریختی از K ــ جبرها مانند*

$$K(G) \cong Mat_{n_1}K \times \cdots \times Mat_{n_t}K$$

وجود دارند.

برهان. چون G متناهی است ، $K(G)$ یک K ــ جبر با بعد متناهی است ؛ و درنتیجه ، آرتینی چپ می‌باشد (تمرین ۲) . حال قضیهٔ ۷.۵ و حکم ۸.۵ را به‌کار برید.

تمرینات

تذکر. K همواره حلقه‌ای تعویضپذیر و یکدار و A یک K ــ جبر است.

۱ . Q ــ جبر A در تمرین IV ۴.۷۰ یک Q ــ جبرآرتینی‌چپ است که حلقهٔ آرتینی چپ *نمی‌باشد*.

۲ . یک جبر با بعد متناهی روی میدان K در هر دو شرط‌زنجیر افزایشی و کاهشی بر ایده‌آلهای جبر چپ و راست صدق می‌کند.

۳ . (آ) هرگاه M یک جبر A ــ مدول چپ باشد ، آنگاه { به‌ازای هر $c \in M$ ، $\mathcal{Q}(M) = \{r \in A \mid rc = 0$ یک ایده‌آل جبر A است.

(ب) ایده‌آل جبری P از A را *اولیه* گویند اگر جبر خارج‌قسمتی R/P اولیه باشد (یعنی ، دارای یک جبر R/P ــ مدول سادهٔ وفادار باشد) . نشان دهید که هر ایده‌آل جبر اولیه یک ایده‌آل اولیهٔ حلقهٔ A است و بالعکس.

۴ . فرض کنید M یک جبر A ــ مدول ساده باشد .

(آ) $D = \mathrm{Hom}_A(M,M)$ یک جبر بخشی روی K است ، که در آن $\mathrm{Hom}_A(M,M)$ تمام درونریختیهای جبر A ــ مدول M می‌باشد .

(ب) M یک جبر D ــ مدول چپ است .

(پ) حلقهٔ $\mathrm{Hom}_D(M,M)$ مرکب از تمام درونریختیهای D ــ جبر از M یک K ــ جبر است .

(ت) نگاشت $r \mapsto \alpha_r$ داده شده با $A \to \mathrm{Hom}_D(M,M)$ (که $\alpha_r(x) = rx$) یک همریختی K ــ جبرهاست .

۵ . فرض کنید A مجموعهٔ تمام ماتریسهای شمارشپذیر نامتناهی روی میدان K باشد (یعنی ، ماتریسهایی‌که سطرها و ستونهایشان با $\mathbf{N}^*$ اندیسگذاری شده‌اند) که فقط تعدادی متناهی درایهٔ ناصفر دارند .

(آ) A یک K ــ جبر ساده است .

(ب) A یک K ــ جبر جبری با بعد نامتناهی است .

۶ . رادیکال J از جبر جبری A روی میدان K پوچ است . [**راهنمایی .** هرگاه $r \in J$ و $k_n r^n + k_{n-1} r^{n-1} + \cdots + k_t r^t = 0$ $(k_t \neq 0)$ ، آنگاه $r^t = r^t u$ که در آن $u = -k_t^{-1} k_n r^{n-t} - \cdots - k_t^{-1} k_{t+1} r$ ، که‌ازآنجا u ــ منتظم‌نمای راست است ؛ مثلا " ، $-u + v - uv = 0$. نشان دهید که $r^t(-u + v - uv) = -r^t = 0$.]

۷ . فرض کنید A یک K ــ جبر بوده و C مرکز حلقهٔ A باشد .

(آ) C یک K ــ زیر جبر A است .

(ب) هرگاه K یک میدان به‌طور جبری بسته بوده و A نیمه ساده با بعد متناهی باشد ، آنگاه تعداد t مولفه‌های سادهٔ A (همانند در قضیهٔ ۷.۵) درست مساوی $\dim_K C$ است .

۶ جبرهای بخشی

ابتدا بعضی ازجبرهای‌ساده‌روی‌یک‌میدان را درنظر گرفته و سپس به حالت خاص جبرهای بخشی روی یک میدان می‌پردازیم . نشان می‌دهیم که ساختار یک جبر بخشی تا حدود زیادی از زیرمیدانهای ماکزیمالش‌تاثیر پذیرفته است . بالاخره ، قضیهٔ نوتر ــ اسکولم [1]

1. Skolem

(۷۰۶) ثابت‌خواهدشد. ازاین دو قضیهٔ مشهور نتیجه می‌شوند که به ترتیب به فروبینوس[1] و ودربورن‌منسوبند (نتایج ۸۰۶ و ۹۰۶) . ضرب تانسوری جبرها (بخش IV ۷۰) به‌طور گسترده‌ای در این بخش به کار خواهد رفت .

تعریف ۱۰۶ . گوییم جبریکدار A روی‌میدان K *سادهٔ مرکزی* است اگر A یک K ــ جبر ساده بوده و مرکز A دقیقا "K باشد .

مثال . فرض کنیم D یک حلقهٔ‌بخشی‌بوده و K مرکز D باشد . به‌آسانی تحقیق می‌شود که هرگاه d عنصر ناصفری از K باشد ، آنگاه $d^{-1} \in K$. درنتیجه ، K یک میدان است . واضح است که D یک جبر روی K است (که K با ضرب معمولی در D عمل می‌کند) . به علاوه ، چون D یک حلقهٔ سادهٔ یکدار است ، به عنوان جبر نیز ساده می‌باشد . لذا ، D یک جبر سادهٔ مرکزی روی K می‌باشد .

به یاد آورید که هرگاه A و B ، K ــ جبرهایی یکدار باشند ، آنگاه حاصل‌ضرب تانسوری آنها $A \otimes_K B$ نیز چنین است (قضیهٔ IV ۴۰۷۰) . حاصل‌ضرب $a \otimes b$ و $a_1 \otimes b_1$ مساوی $aa_1 \otimes bb_1$ است . دراینجاو ذیلا "مجموعهٔ" $\{1_A \otimes b \mid b \in B\}$ را با $1_A \otimes_K B$ و $\{a \otimes 1_B \mid a \in A\}$ را با $A \otimes_K 1_B$ نشان می‌دهیم . توجه کنید که

$$A \otimes_K B = (A \otimes_K 1_B)(1_A \otimes_K B)$$

ر.ک. ص ۳۵۸ .

قضیهٔ ۲۰۶ . هرگاه A یک جبر سادهٔ مرکزی روی میدان K بوده و B یک K ــ جبر یکدار باشد ، آنگاه $A \otimes_K B$ یک K ــ جبر ساده خواهد بود .

برهان . چون B یک فضای برداری روی K است ، پایه‌ای چون Y دارد و ، بنابر قضیهٔ IV ۱۱۰۵۰ ، هر عنصر u از $A \otimes_K B$ را می‌توان به صورت $\sum_{i=1}^{n} a_i \otimes y_i$ نوشت ، که در آن $y_i \in Y$ ها و a_i ها منحصربه‌فردند . اگر U ایده‌آل ناصفری از $A \otimes_K B$ باشد ، عنصر ناصفری چون $u \in U$ وجوددارد‌به‌طوری که $u = \sum_{i=1}^{n} a_i \otimes y_i$ ، که درآن همهٔ a_i ها ناصفر

1. Frobenius

بوده و n مینیمال است. چون A ساده و یکدار است و Aa_1A ایده‌آل ناصفر است، $Aa_1A = A$. درنتیجه، عناصری چون $r_1, \ldots, r_t, s_1, \ldots, s_t \in A$ وجود دارند به‌طوری که $1_A = \sum_{j=1}^{t} r_j a_1 s_j$. چون U ایده‌آل است، عنصر $v = \sum_{j=1}^{t} (r_j \otimes 1_B)u(s_j \otimes 1_B)$ درمجموعهٔ U است. اما

$$v = \sum_j (r_j \otimes 1_B)(\sum_i a_i \otimes y_i)(s_j \otimes 1_B) = \sum_i (\sum_j r_j a_i s_j) \otimes y_i$$
$$= \sum_j r_j a_1 s_j \otimes y_1 + \sum_{i=2}^{n} (\sum_j r_j a_i s_j) \otimes y_i = 1_A \otimes y_1 + \sum_{i=2}^{n} \bar{a}_i \otimes y_i,$$

که در آن $\bar{a}_i = \sum_{j=1}^{t} r_j a_i s_j$. بنابر مینیمالی n، به‌ازای هر $i \geq 2$، $\bar{a}_i \neq 0$. هرگاه $a \in A$، آنگاه عنصر $w = (a \otimes 1_B)v - v(a \otimes 1_B)$ در U است و

$$w = \left(a \otimes y_1 + \sum_{i=2}^{n} a\bar{a}_i \otimes y_i\right) - \left(a \otimes y_1 + \sum_{i=2}^{n} \bar{a}_i a \otimes y_i\right)$$
$$= \sum_{i=2}^{n} (a\bar{a}_i - \bar{a}_i a) \otimes y_i.$$

بنابر مینیمالی n، $w = 0$ و به‌ازای هر $i \geq 2$، $a\bar{a}_i - \bar{a}_i a = 0$. لذا، به‌ازای هر $a \in A$، $a\bar{a}_i = \bar{a}_i a$ و هر $\bar{a}_i$ در مرکز A است، که طبق فرض درست مساوی K می‌باشد. بنابراین،

$$v = 1_A \otimes y_1 + \sum_{i=2}^{n} \bar{a}_i \otimes y_i = 1_A \otimes y_1 + \sum_{i=2}^{n} 1_A \otimes \bar{a}_i y_i = 1_A \otimes b,$$

که در آن $b = y_1 + \bar{a}_2 y_2 + \cdots + \bar{a}_n y_n \in B$. چون هر $\bar{a}_i \neq 0$ و y_i ها روی K مستقل خطی‌اند، $b \neq 0$. لذا، چون B یکدار است، بنابر سادگی، ایده‌آل BbB درست مساوی B می‌باشد. بنابراین،

$$1_A \otimes_K B = 1_A \otimes BbB = (1_A \otimes_K B)(1_A \otimes b)(1_A \otimes_K B)$$
$$= (1_A \otimes_K B)v(1_A \otimes_K B) \subset U.$$

درنتیجه،

$$A \otimes_K B = (A \otimes_K 1_B)(1_A \otimes_K B) \subset (A \otimes_K 1_B)U \subset U.$$

بنابراین، $U = A \otimes_K B$ و فقط یک ایده‌آل ناصفر از $A \otimes_K B$ وجود دارد. چون $A \otimes_K B$

دارای واحد $1_A \otimes 1_B$ است، $(A \otimes_K B)^2 \neq 0$، که از آنجا $A \otimes_K B$ ساده می‌باشد.

حال حلقه‌های بخشی را درنظر می‌گیریم. اگر D یک حلقهٔ بخشی بوده و F زیرحلقه‌ای از D شامل 1_D باشد که میدان است، F یک ***زیرمیدان*** D نام دارد. واضح است که D یک فضای برداری روی هر زیرمیدان F است. زیرمیدان F از D را یک ***زیرمیدان ماکزیمال*** گوییم اگرحقیقتا" مشمول زیرمیدان دیگری از D نباشد. زیرمیدانهای ماکزیمال همیشه وجود دارند (تمرین ۴). هر زیرمیدان ماکزیمال F از D شامل مرکز K از D است (در غیر این صورت، F و K زیرمیدانی از D را تولید می‌کنند که حقیقتا" شامل F است؛ تمرین ۳). به‌آسانی معلوم می‌شود که F درواقع یک K ــ جبر ساده است. زیرمیدانهای ماکزیمال یک حلقهٔ بخشی بر ساختار خود حلقهٔ بخشی اثر بسیار دارند، و این در قضایای زیر نموده خواهد شد.

قضیهٔ ۳۰۶. ***فرض کنیم D یک حلقهٔ بخشی به مرکز K بوده و F زیرمیدان ماکزیمالی از D باشد. دراین‌صورت، $D \otimes_K F$ (به‌عنوان Kـجبر) با زیرجبر چگالی از $Hom_K(D,D)$ یکریخت است، که در آن D یک فضای برداری روی F درنظر گرفته می‌شود.***

برهان. $\mathrm{Hom}_F(D,D)$ یک F ــ جبر است (سومین مثال پس از تعریف IV ۱.۷۰)؛ و درنتیجه، یک K ــ جبر می‌باشد. به‌ازای هر $a \in D$، فرض کنیم $\alpha_a : D \to D$ با $\alpha_a(x) = xa$ تعریف‌شده باشد. به‌ازای هر $c \in F$، فرض کنیم $\beta_c : D \to D$ با $\beta_c(x) = cx$ تعریف شده باشد. تحقیق کنید که به‌ازای هر $a \in D, c \in F$، $\alpha_a, \beta_c \in \mathrm{Hom}_F(D,D)$ و $\alpha_a\beta_c = \beta_c\alpha_a$. و نیز تحقیق کنید که نگاشت $D \times F \to \mathrm{Hom}_F(D,D)$ داده شده با $(a,c) \mapsto \alpha_a\beta_c$، K ــ دوخطی است. بنابر قضیهٔ IV ۶.۵۰، این نگاشت یک همریختی K ــ مدولها مانند $\theta : D \otimes_K F \to \mathrm{Hom}_F(D,D)$ القا می‌کند به‌طوری که

$$\theta\left(\sum_{i=1}^{n} a_i \otimes c_i\right) = \sum_{i=1}^{n} \alpha_{a_i}\beta_{c_i} \quad (a_i \in D,\ c_i \in F).$$

تحقیق کنیدکه θ یک‌همریختی K ــ جبرهاست، که صفر نیست (زیرا $\theta(1_D \otimes 1_D)$ نگاشت همانی بر D است). چون D یک سادهٔ مرکزی بوده و F یک K ــ جبر ساده است، بنابر قضیهٔ ۲.۶، $D \otimes_K F$ ساده می‌باشد. چون $\theta \neq 0$ و $\mathrm{Ker}\ \theta$ یک ایده‌آل جبر است،

$\operatorname{Ker}\theta = 0$ ، که ازآنجا θ یک تکریختی است. بنابراین ، $D \otimes_K F$ با K ــ زیرجبر $\operatorname{Im}\theta$ از $\operatorname{Hom}_F(D,D)$ یکریخت است. باید نشان دهیم که $A = \operatorname{Im}\theta$ در $\operatorname{Hom}_F(D,D)$ چگال است.

D بوضوح یک مدول چپ روی $\operatorname{Hom}_F(D,D)$ است که در آن داریم $fd = f(d)$ $(f \in \operatorname{Hom}_F(D,D), d \in D)$. درنتیجه ، D یک مدول چپ روی $A = \operatorname{Im}\theta$ می‌باشد. هرگاه d عنصر ناصفری از D باشد ، آنگاه چون D حلقهٔ بخشی است ،

$$Ad = \{\theta(u)(d) \mid u \in D \otimes_K F\} = \{\sum_i c_i d a_i \mid i \in \mathbf{N}^*;\ c_i \in F;\ a_i \in D\} = D.$$

درنتیجه ، D دارای A ــ زیرمدول نابدیهی نیست؛ درنتیجه ، D یک A ــ مدول ساده می‌باشد. به علاوه ، D یک A ــ مدول وفادار است ، زیرا نگاشت صفر تنها عنصر f از $\operatorname{Hom}_F(D,D)$ است که $fD = 0$. بنابراین ، طبق قضیهٔ چگالی ۱۲۰۱ ، A با زیرحلقهٔ چگالی از $\operatorname{Hom}_\Delta(D,D)$ یکریخت است ، که در آن Δ حلقهٔ بخشی $\operatorname{Hom}_A(D,D)$ بوده و D یک Δ ــ فضای برداری چپ می‌باشد. تحت تکریختی $A \to \operatorname{Hom}_\Delta(D,D)$ ، نقش $f \in A$ مساوی f است که به عنوان عنصری از $\operatorname{Hom}_\Delta(D,D)$ درنظر گرفته شود.

حال یکریختی $F \cong \Delta$ از حلقه‌ها را می‌سازیم . فرض کنیم $\beta : F \to \Delta = \operatorname{Hom}_A(D,D)$ با $c \mapsto \beta_c$ داده شده باشد (نمادها مثل بالا) . تحقیق کنید که $\beta_c \in \Delta$ و β یک تکریختی حلقه‌هاست. هرگاه $f \in \Delta$ و $x \in D$ ، آنگاه $\alpha_x = \theta(x \otimes 1_D) \in A$ و

$$f(x) = f(1_D x) = f[\alpha_x(1_D)] = \alpha_x(f(1_D)) = f(1_D)x = \beta_c(x),$$

که در آن $c = f(1_D)$. برای نشان دادن اینکه β برووریختی است ، کافی است ثابت شود که $c \in F$ ؛ زیرا در این حالت ، به‌ازای هر $x \in D$ ، $f(x) = cx = \beta_c(x)$ ، که از آنجا $f = \beta_c = \beta(c)$. هرگاه $y \in F$ ، آنگاه $\beta_y = \theta(1_D \otimes y) \in A$ و $\alpha_y = \theta(y \otimes 1_D) \in A$ و

$$\begin{aligned} cy &= f(1_D)y = \alpha_y(f(1_D)) = f(\alpha_y(1_D)) = f(1_D y) = f(y 1_D) \\ &= f(\beta_y(1_D)) = \beta_y f(1_D) = \beta_y(c) = yc. \end{aligned}$$

بنابراین ، c با هر عنصر F تعویض می‌شود. هرگاه $c \notin F$ ، آنگاه c و F زیرمیدانی از D تولید می‌کنندکه حقیقتا" شامل زیرمیدان ماکزیمال F است (تمرین ۳) . چون این یک تناقض است ، باید داشته باشیم $c \in F$. بنابراین ، $\beta : F \cong \Delta$.

برای اتمام برهان ، فرض کنیم $v_1, \ldots, v_n \in D$ و $\{u_1, \ldots, u_n\}$ زیرمجموعه‌ای از D

باشد که روی F مستقل‌خطی‌است. حکم می‌کنیم که $\{u_1, \ldots, u_n\}$ روی Δ نیز مستقل خطی است. هرگاه $(g_i \in \Delta) \sum_{i=1}^{n} g_i u_i = 0$، آنگاه

$$0 = \sum g_i u_i = \sum \beta_{c_i}(u_i) = \sum c_i u_i,$$

که در آن $c_i \in F$ و $g_i = \beta(c_i) = \beta_{c_i}$. F ــ استقلال خطی $\{u_1, \ldots, u_n\}$ ایجاب می‌کندکه هر $c_i = 0$، که از آنجـا به‌ازای هر i، $g_i = \beta(0) = 0$. بنابراین، $\{u_1, \ldots, u_n\}$ روی Δ مستقل خطی است. بنابر چگال بودن A در $\mathrm{Hom}_\Delta(D,D)$ (تعریف ۷۰۱)، $h \in A$ ی هست‌به‌طوری‌که‌به‌ازای‌هر i، $h(u_i) = v_i$. بنابراین، A در $\mathrm{Hom}_F(D,D)$ چگال می‌باشد.

قضیهٔ ۳۰۶ دارای نتیجهٔ جالبی است که به دو لم مقدماتی نیاز دارد.

لم ۴۰۶ . فرض کنیم A یک جبریکدار روی‌میدان K بوده و F میدانی شامل K باشد؛ در این صورت، $A \otimes_K F$ یک F ــ جبر است به‌طوری که $\dim_K A = \dim_F(A \otimes_K F)$.

طرح برهان. چون F تعـویضپذیر و K-F دو مدول است، $A \otimes_K F$ فضایی برداری روی F اسـت کـه در آن $b(a \otimes b_1) = (a \otimes b_1)b = a \otimes b_1 b$ ($a \in A; b, b_1 \in F$)؛ ر.ک. قضیهٔ IV ۵۰۵۰ وتبصرهٔ‌بعدازآن) . بنابر قضیهٔ IV ۴۰۷۰، $A \otimes_K F$ یک K ــ جبر است و به‌آسانی معلوم می‌شود که یک F ــ جبر نیز هست. هرگاه X یک پایهٔ A روی K باشد، آنگاه، بنابر (مشابه بدیهی) قضیهٔ IV ۱۱۰۵۰، هر عنصر $A \otimes_K F$ را می‌توان به صورت زیر نوشت:

$$\sum_i x_i \otimes c_i = \sum_i (x_i \otimes 1_F)c_i = \sum_i c_i(x_i \otimes 1_F) \quad (x_i \in X; c_i \in F),$$

که در آن عناصر x_i و c_i به‌طور منحصر به فرد معین می‌شوند. لذا، نتیجه می‌شود کـه

$$X \otimes_K 1_F = \{x \otimes 1_F \mid x \in X\}$$

یک پایهٔ $A \otimes_K F$ روی F است. واضح است که

$$\dim_K A = |X| = |X \otimes_K 1_F| = \dim_F(A \otimes_K F) .$$

لم ۵۰۶ . فرض کنیم D یک جبـر بخشی روی میدان K بوده و A یک K ــ جبر با بعد

متناهی و یکدار باشد. در این صورت، $D \otimes_K A$ یک K ــ جبر آرتینی چپ است.

طرح برهان. $D \otimes_K A$ یک‌فضای‌برداری‌روی D است که عمل $d \in D$ بر مولـد $d_1 \otimes a$ از $D \otimes_K A$ با $d(d_1 \otimes a) = dd_1 \otimes a = (d \otimes 1_A)(d_1 \otimes a)$ داده‌می‌شود (قضیهٔ IV ۵۰۵۰). درنتیجه، هر ایده‌آل چپ $D \otimes_K A$ یک D ــ زیرفضای $D \otimes_K A$ نیز می‌باشد. در اینجا برهان لم ۴۰۶ **نعل به نعل** برقرار است و نشـان می‌دهد که $\dim_D(D \otimes_K A) = \dim_K A$. چون $\dim_K A$ متناهی‌است، استدلال‌معمول در باب بعد نشان می‌دهد که $D \otimes_K A$ آرتینی چپ می‌باشد.

قضیهٔ ۶۰۶. فرض‌کنیم D یک حلقهٔ بخشی به مرکز K و زیرمیدان ماکزیمال F باشد. در این صورت، $\dim_K D$ متناهی‌است‌اگر و فقط‌اگر $\dim_K F$ متناهی باشد، که در این‌صورت $\dim_K D = (\dim_K F)^2$ و $\dim_F D = \dim_K F$.

برهان. اگر $\dim_K F$ نامتناهی‌باشد، $\dim_K D$ نیزچنین‌است. هرگاه $\dim_K F$ متناهی باشد، آنگاه، بنـابر لـم ۵۰۶، $D \otimes_K F$ یک K ــ جبر آرتینی چپ است. لذا، طبق قضیهٔ ۳۰۶، $D \otimes_K F$ با زیرجبر آرتینـی چپ چگالی از $\mathrm{Hom}_F(D,D)$ یکریخت است. برهان قضیهٔ ۳۰۶ نشان مـی‌دهد که این یکریختی عملاً "یکریختی F ــ جبرهاست. درنتیجه، یک یکریختی F ــ جبرهامانند $D \otimes_K F \cong \mathrm{Hom}_F(D,D)$ وجوددارد و، بنابرقضیهٔ ۹۰۱، $n = \dim_F D$ متناهی‌می‌باشد. بنابراین، طبق قضیهٔ VII ۴۰۱۰ (و تبصرهٔ بعد از آن)، $D \otimes_K F \cong \mathrm{Hom}_F(D,D) \cong \mathrm{Mat}_n F$. حال لم ۴۰۶ ایجاب می‌کند که

$$\dim_K D = \dim_F(D \otimes_K F) = \dim_F(\mathrm{Mat}_n F) = n^2 = (\dim_F D)^2.$$

از آن سو، طبق قضیهٔ IV ۱۶۰۲۰، $\dim_K D = (\dim_F D)(\dim_K F)$. بنابراین،

$$\dim_K F = \dim_F D.$$

به یاد آورید که هرگاه u یک یکه در حلقـهٔ یکدار R باشد، آنگاه نگاشت $R \to R$ داده شده با $r \mapsto uru^{-1}$ یک‌خودریختی‌حلقهٔ R است. این‌خودریختی **خودریختی داخلی** القا شده به وسیلهٔ u نام دارد.

قضیهٔ ۷۰۶. (نوتر ــ اسکولم) فرض‌کنیم R یک حلقهٔ آرتینی چپ ساده بوده و K

مرکز R باشد (درنتیجه، R یک K ــ جبراست). همچنین، A و B، K ــ زیرجبرهای ساده با بعد متناهی از R باشند که شامل K اند. هرگاه $\alpha : A \to B$ یک یکریختی K ــ جبرها باشد که K را عنصروار ثابت می‌گذارد، آنگاه α به یک خودریختی داخلی R توسیع می‌یابد.

برهان. بنابر قضیهٔ ودربورن ــ آرتین ۱۴۰۱، فرض می‌کنیم $R = \mathrm{Hom}_D(V,V)$، که در آن V یک فضای برداری n بعدی روی حلقهٔ بخشی D است. تبصره‌های بعد از قضیهٔ VII ۳۰۱۰ نشان می‌دهند که یک پادیکریختی حلقه‌ها مانند $R = \mathrm{Hom}_D(V,V) \to \mathrm{Mat}_n D$ وجوددارد. تحت این نگاشت، مرکز K ی R لزوماً **به‌طور یکریخت** به روی مرکز $\mathrm{Mat}_n D$ نگاشته می‌شود. اما، بنابر تمرین VII ۳۰۱۰، مرکز $\mathrm{Mat}_n D$ با مرکز D یکریخت است. درنتیجه، K را با مرکز D یکی می‌کنیم؛ درنتیجه، D یک K ــ جبرسادهٔ مرکزی می‌باشد.

توجه کنید که V یک K ــ مدول چپ است که در آن $(v \in V; r \in R = \mathrm{Hom}_D(V,V))\ rv = r(v)$. چون V یک D ــ فضای برداری چپ است، نتیجه می‌شود که V یک مدول جبر چپ روی K ــ جبر $D \otimes_K R$ است، که در آن عمل مولد $d \otimes r$ از $D \otimes_K R$ بر $v \in V$ به صورت زیر داده می‌شود:

$$(d \otimes r)v = d(rv) = d(r(v)) = r(dv). \qquad \text{(یک)}$$

هرگاه $\bar{A}$ زیر جبر $D \otimes_K A$ از $D \otimes_K R$ باشد، آنگاه V بوضوح یک $\bar{A}$ ــ مدول چپ است. به همین نحو، هرگاه $\bar{B} = D \otimes_K B$، آنگاه V یک $\bar{B}$ ــ مدول چپ است. اما نگاشت $\bar{\alpha} = 1_D \otimes \alpha : \bar{A} \to \bar{B}$ یک یکریختی K ــ جبرهاست. درنتیجه، V دارای ساختار $\bar{A}$ ــ مدول دومی است که به وسیلهٔ برگشت در امتداد $\bar{\alpha}$ داده می‌شود (یعنی، به‌ازای $v \in V, \bar{a} \in \bar{A}$، $\bar{a}v$ مساوی $\bar{\alpha}(\bar{a})v$ تعریف می‌شود؛ ر.ک. ص ۲۶۵). تحت این ساختار $\bar{A}$ ــ مدول دوم، عمل مولد $d \otimes r$ از $\bar{A} = D \otimes_K A$ بر $v \in V$ با

$$(d \otimes r)v = \bar{\alpha}(d \otimes r)v = (d \otimes \alpha(r))v = d(\alpha(r)(v)) = \alpha(r)(dv) \qquad \text{(دو)}$$

داده می‌شود.

بنابرقضیهٔ ۲۰۶ و لم ۵۰۶، $\bar{A}$ یک K ــ جبر آرتینی چپ ساده است. درنتیجه، طبق قضیهٔ ۱۰۰۳، فقط یک $\bar{A}$ ــ مدول ساده (با تقریب یکریختی) وجود دارد. اما، بنابرقضیهٔ ۷۰۳، V با ساختار $\bar{A}$ ــ مدول (یک) یا (دو) نیمه ساده است. درنتیجه، یکریختیهای $\bar{A}$ ــ مدولهای

$$V = \sum_{i\in I} U_i \quad \text{(نظیر به ساختار (یک))} \qquad \text{(سه)}$$

و

$$V = \sum_{j\in J} W_j \quad \text{(نظیر به ساختار (دو))} \qquad \text{(چهار)}$$

وجود دارند، که در آنها هر U_i, W_i یک $\bar{A}$ ــ مدول ساده است و به‌ازای هر i,j ، $U_i \cong W_j$. چون $(d\in D, v\in V)\ dv = (d\otimes 1_R)v$ ، هر $\bar{A}$ ــ زیرمدول V یک D ــ زیرفضای V است و هر یکریختی $\bar{A}$ ــ مدولها یک یکریختی D ــ فضاهای برداری است . چون $\dim_D V = n$ متناهی است، هر U_i, W_i دارای بعد متناهی t روی D است و مجموعه‌های اندیسگذار I, J متناهی می‌باشند؛ مثلا" ،

$$I = \{1,2,\ldots,m\} \quad \text{و} \quad J = \{1,2,\ldots,s\} .$$

بنابراین ،

$$\dim_D V = \dim_D \left(\sum_{i=1}^{m} U_i\right) = \sum_{i=1}^{m} \dim_D U_i = mt,$$

و

$$\dim_D V = \dim_D \left(\sum_{j=1}^{s} W_j\right) = \sum_{j=1}^{s} \dim_D W_j = st,$$

که از آنجا $m = s$. چون به‌ازای هر i,j ، $U_i \cong W_j$ ، $\sum_{i=1}^{m} U_i \cong \sum_{j=1}^{m} W_j$. از تلفیق این یکریختی با یکریختیهای (سه) و (چهار) فوق ، یکریختی $\bar{A}$ ــ مدولها مانند β از V (با ساختار $\bar{A}$ ــ مدولهای (یک)) و V (با ساختار $\bar{A}$ ــ مدولهای (دو)) به دست می‌آید . لذا ، به‌ازای هر $\bar{a}\in\bar{A}$ و $v\in V$ ،

$$\beta(\bar{a}v) = \bar{\alpha}(\bar{a})(\beta(v)).$$

بخصوص، به‌ازای $d\in D$ و $\bar{d} = d\otimes 1_A \in \bar{A}$ ،

$$\beta(dv) = \beta(\bar{d}v) = \bar{\alpha}(\bar{d})(\beta(v)) = (d\otimes 1_B)\beta(v) = d\beta(v),$$

که از آنجا $\beta\in \mathrm{Hom}_D(V,V) = R$. چون β یکریختی است، β یک یکه در R است . به علاوه، به‌ازای $r\in A$ و $\bar{r} = 1_D\otimes r\in\bar{A}$ ،

$$\begin{aligned}\beta r(v) &= \beta[r(v)] = \beta[\bar{r}v] = \bar{\alpha}(\bar{r})\beta(v)\\ &= (1_D\otimes\alpha(r))\beta(v) = \alpha(r)[\beta(v)] = [\alpha(r)\beta](v),\end{aligned}$$

که از آنجا $\beta r = \alpha(r)\beta$ در $R = \mathrm{Hom}_D(V,V)$ است. به عبارت دیگر ،

به‌ازای هر $r\in A$ ، $\beta r\beta^{-1} = \alpha(r)$.

بنابراین ،خودریختی داخلی R القاشده‌بوسیلهٔ β به‌نگاشت $\alpha : A\to\bar{B}$ توسیع می‌یابد.

جبربخشی‌چهارتاهای‌حقیقی ،که درنتیجهٔ بعد ذکر شده ، در صفحات ۱۸۲ و ۳۵۵ تعریف شده است .

نتیجهٔ ۸.۶ (فروبینوس) . *فرض‌کنیم* D *یک جبر بخشی جبری روی میدان اعداد حقیقی* R *باشد . در این صورت ،* D *با* R *یا میدان اعداد مختلط* C *یا جبر بخشی چهارتاهای حقیقی* T *یکریخت است .*

طرح برهان . فرض‌کنیم K مرکز D و F یک زیرمیدان ماکزیمال باشد . داریم $\mathbf{R} \subset K \subset F \subset D$ ، که درآن F یک‌توسیع میدان جبری از $\mathbf{R}$ است . لذا ، طبق نتیجهٔ ۲۰.۳۰.۷ ، $\dim_K F \leq \dim_{\mathbf{R}} F \leq 2$. بنابر قضیهٔ ۶.۶ ، $\dim_F D = \dim_K F$ و $\dim_K D = (\dim_K F)^2$. لذا ،تنهاامکانات عبارتند از $\dim_K D = 1$ و $\dim_K D = 4$. هرگاه $\dim_K D = 1$ ، آنگاه $D = F$ ، و D طبق نتیجهٔ ۲۰.۳۰.۷با $\mathbf{R}$ یابا $\mathbf{C}$ یکریخت‌است .

هرگاه $\dim_K D = 4$ ، آنگاه $\dim_K F = 2 = \dim_F D$ ، که از آنجا $K = \mathbf{R}$ و F طبق نتیجهٔ ۲۰.۳۰.۷ با $\mathbf{C}$ یکریخت‌است . به علاوه ، D تعویض‌ناپذیر است . در غیر این صورت ، D یک توسیع میدان جبری حقیقی از میدان به‌طور جبری بستهٔ $\mathbf{C}$ خواهد بود . چون F با $\mathbf{C}$ یکریخت‌است ، به‌ازای $i \in F$ ی که $i^2 = -1$ ، $F = \mathbf{R}(i)$. نگاشت $F \to F$ داده شده با $a + bi \mapsto a - bi$ یک خودریختی‌غیرهمانی F است که $\mathbf{R}$ را عنصروار ثابت نگه می‌دارد . بنابر قضیهٔ ۷.۶ ، آن به یک خودریختی داخلی مانند β از D توسیع می‌یابد که ، به‌ازای عنصر ناصفری چون $d \in D$ ، با $\beta(x) = dxd^{-1}$ داده می‌شود .

ازآنجاکه $-i = \beta(i) = did^{-1}$ ، داریم $-id = di$ ؛ و درنتیجه ، $id^2 = d^2 i$. درنتیجه ، $d^2 \in D$ با هر عنصر $F = \mathbf{R}(i)$ تعویض می‌شود . بنابراین ، $d^2 \in F$ ؛ در غیر این صورت ، d^2 و F زیرمیدانی از D را تولید می‌کنند که حقیقتا" مشمول زیرمیدان ماکزیمال F است . چون تنها عناصر F که توسط β ثابت می‌مانند عنصرهای $\mathbf{R}$ و $\beta(d^2) = dd^2d^{-1} = d^2$ اند ،داریم $d^2 \in \mathbf{R}$.هرگاه $d^2 > 0$ ،آنگاه $d \in \mathbf{R}$.این‌ممکن نیست، زیرا $d \in \mathbf{R}$ ایجاب می‌کند که β نگاشت همانی باشد . لذا ، به‌ازای $r \in \mathbf{R}$ ی ناصفر ، $d^2 = -r^2$ ، که از آنجا $(d/r)^2 = -1$. فرض‌کنیم $j = d/r$ و $k = ij$. تحقیق‌کنید که $\{1,i,j,k\}$ پایه‌ای از D روی $\mathbf{R}$ استو یک یکریختی $\mathbf{R}$ ــ جبرها مانند $D \cong \boldsymbol{T}$ موجود خواهد بود.

نتیجهٔ ۹.۶ . (ودربورن) *هر حلقهٔ بخشی متناهی* D *یک میدان است .*

تبصره . برهان مقدماتی این امر ، از طریق چندجمله‌ایهای دایره بر ، در تمرین ۱۰.۸.۷ داده شده است .

برهان ۹.۶ . فرض کنیم K مرکز D و F زیرمیدان ماکزیمالی باشد . بنابر قضیهٔ ۶.۶ ، $\dim_K D = n^2$ ، که در آن $\dim_K F = n$. لذا ، هر زیرمیدان ماکزیمال یک میدان متناهی از مرتبهٔ q^n است ، که در آن $q = |K|$. از اینرو ، هر دو زیرمیدان ماکزیمال F و F' یکریخت‌اند تحت یک یکریختی مانند $\beta : F \to F'$ که K را عنصروارثابت می‌گذارد (نتیجهٔ ۸.۵.۷) . بنابر قضیهٔ ۷.۶ ، β به وسیلهٔ یک خودریختی داخلی D داده می‌شود . لذا ، به‌ازای عنصر ناصفری چون $a \in D$ ، $F' = aFa^{-1}$.

هرگاه $u \in D$ ، آنگاه $K(u)$ زیرمیدانی از D است (تمرین ۳) . $K(u)$ مشمول زیرمیدان ماکزیمالی به شکل aFa^{-1} (به‌ازای $a \in D$ ای) می‌باشد . لذا ، $D = \bigcup_{0 \neq a \in D} aFa^{-1}$ و $D^* = \bigcup_{a \in D^*} aF^*a^{-1}$ (که در آن D^*, F^* به ترتیب گروههای ضربی عناصر ناصفر D, F اند) . بنابر لم ۱۰.۶ زیر ، این ناممکن است مگر اینکه $F = D$.

لم ۱۰.۶ . *هرگاه* G *یک گروه متناهی (ضربی) بوده و* H *یک زیرگروه حقیقی باشد ، آنگاه*

$$\bigcup_{x \in G} xHx^{-1} \subsetneq G.$$

برهان . تعداد مزدوجهای متمایز H مساوی $[G : N]$ است ، که در آن N نرمال‌ساز H در G است (نتیجهٔ ۴.۴.۰ II) . چون $H < N < G$ و $H \neq G$ ، $[G : N] \leq [G : H]$ و $[G : H] > 1$. هرگاه r تعداد عناصر متمایز در $\bigcup_{x \in G} xHx^{-1}$ باشد ، آنگاه

$$\begin{aligned} r &\leq 1 + (|H| - 1)[G : N] \leq 1 + (|H| - 1)[G : H] \\ &= 1 + |H|[G : H] - [G : H] = 1 + |G| - [G : H] < |G|, \end{aligned}$$

زیرا $[G : H] > 1$.

تمرینات

۱ . هرگاه A یک جبر سادهٔ مرکزی با بعد متناهی روی میدان K باشد، آنگاه $A \otimes_K A^{op} \cong \mathrm{Mat}_n K$ ، که در آن $n = \dim_K A$ و A^{op} درتمرین III ۱۷.۱.۰تعریف شده است.

۲ . هرگاه A و B جبرهای سادهٔ مرکزی روی میدان K باشند، آنگاه $A \otimes_K B$ نیز چنین است.

۳ . فرض کنید D یک حلقهٔ بخشی بوده و F یک زیرمیدان باشد. هرگاه $d \in D$ با هر عنصر F تعویض شود، آنگاه حلقهٔ زیر بخشی $F(d)$ که به وسیلهٔ F و d تولید می‌شود (اشتراک تمام حلقه‌های زیربخشی D شامل F و d) یک زیرمیدان است. [ر.ک. قضیهٔ V ۳.۱.۰.]

۴ . هرگاه D یک حلقهٔ بخشی باشد، آنگاه D شامل زیرمیدان ماکزیمال است.

۵ . هرگاه A یک جبر سادهٔ مرکزی با بعد متناهی روی میدان K باشد، آنگاه $\dim_K A$ مجذور کامل است.

۶ . هرگاه A و B جبرهای آرتینی چپ روی میدان K باشد، آنگاه $A \otimes_K B$ لازم نیست آرتینی چپ باشد. [**راهنمایی** . فرض کنید A یک جبر بخشی به مرکز K و زیرمیدان ماکزیمال B باشد به‌طوری که $\dim_B A$ نامتناهی است.]

۷ . هرگاه D جبر بخشی با بعد متناهی روی مرکزش K بوده و F زیرمیدان ماکزیمالی از D باشد، آنگاه یک یکریختی K ــ جبرها مانند $D \otimes_K F \cong \mathrm{Mat}_n F$ وجود دارد، که در آن $n = \dim_F D$.

۸ . هرگاه A یک جبرساده و بابعد متناهی روی مرکزش باشد، آنگاه هر خودریختی A که مرکز را عنصروار ثابت بگذارد یک خودریختی داخلی است.

۹ . (دیکسون[1]) فرض کنید D یک حلقهٔ بخشی به مرکز K باشد. هرگاه $a,b \in D$ روی میدان K جبری بوده و چندجمله‌ای مینیمال یکسانی داشته باشند، آنگاه، به‌ازای $d \in D$ ای، $b = dad^{-1}$.

---

1. Dickson

۱۰

رسته‌ها

در ایـن فصـل آشنایی با نظریهٔ رسته‌ها، که در بخش I ۷۰ آغاز شد، کامل می‌شود. رسته‌ها و تـابعگرها اول بـار در دههٔ ۱۹۴۰ در کارهای ایلنبرگ[1] ــ مک‌لین در توپولوژی جبری‌ظاهرشدند. بزودی معلوم شد که این مفاهیم کاربردهای بسیار گسترده‌تری دارند. بسیاری‌ازمباحث‌مختلف‌ریاضی را می‌توان برحسب رسته‌ها تعبیر کرد؛ درنتیجه، تکنیکها و قضایای نظـریهٔ رستـه‌ها را می‌توان در این مباحث به کار برد. مثلا"، دو برهان در حیطه‌های‌جدااز هم مکرر از روشهای "مشابه" استفاده می‌کنند. جبر رسته‌ای ابزار دقیق بیان این تشابهات را فراهم می‌سازد. درنتیجه، بسیار اتفاق می‌افتد که برهانی در یک محدودهٔ رسته‌ای بـه دست می‌آید که حالات خـاصی از آن نتایج معلومی در دو حیطهٔ مختلف می‌باشند. این فرایند یکی‌سازی ابزار درک حیطه‌های وسیعتری از ریاضیات و نیز مباحث جدیدی که مبانی آنها با اصطلاحات رسته قابل بیانند را به ما خواهد داد.

در این کتاب نظریهٔ رسته‌ها عمدتا" به همین منظور به کار می‌رود ــ زبان مناسبی برای یکی‌سازی. امادر سالهای اخیر نظریهٔ رسته‌ها خود به عنوان یک نظام ریاضی ظاهر شده‌است. اکنون منابع الهام برای پیشرفت در نظریهٔ رسته‌ها اغلب از خود نظریه نشأت می‌گیرند. در این فصل فقط به این گسترش اشاره شده است.

مفاهیم اساسی تابعگروتبدیل طبیعی به‌طورکامل در بخش ۱ مطرح شده‌اند. دو نوع تابعگرکه ازاهمیت خاصی برخوردارند عبارتند از تابعگر نمایشپذیر (بخش ۱) و جفتهای الحاقی‌ازتابعگرها (بخش۲). بخش ۳ اختصاص به انتقال هرچه بیشتر مفاهیم از رسته‌های مشهور، نظیر رستهٔ مدولها روی یک حلقه، به رسته‌های دلخواه دارد.

1. Eilenberg

این فصل به بخش I ۷۰ وابسته است ولی از بقیهٔ کتاب، جز چند مثال، مستقل می‌باشد. بخشهای ۱ و ۳ اساسا" مستقل می‌باشند. بخش ۱ پیشنیاز بخش ۲ می‌باشد.

۱ تابعگرها و تبدیلات طبیعی

همانطور که در فصول قبل کرارا" دیده‌ایم، مطالعهٔ اشیاء ریاضی نیاز به توجه به"نگاشتهای" این اشیاء دارد. درحالت‌فعلی، اشیاء ریاضی‌مورد بحث رسته‌هامی‌باشند (بخش I ۷۰). یک تابعگر را می‌توان به‌طور نادقیق "نگاشتی" توصیف کرد از یک رسته به رستهٔ دیگرکه ساختار مناسبی‌را حفظ‌کند. یک تبدیل طبیعی، به نوبهٔ خود، "نگاشتی" از یک تابعگر به تابعگر دیگر است.

با تعریف تـابعگرهای همـورد و پـادورد و چند مثال از آنها آغاز می‌کنیم. سپس تبدیلات طبیعی معرفی شده و چند مثال دیگر خواهیم آورد. آخرین قسمت بخش به‌چند تابعگر مهم در نظریهٔ رسته‌ها، یعنی تابعگرهای نمایشپذیر، اختصاص یافته است.

لازم‌است‌خواننده‌خواص اساسی رسته‌ها (بخش I ۷۰)، بخصوص مفهوم شیء عمومی (که‌درمطالعهٔ تابعگرهای نمایشپذیر لازم می‌شود)، را مرور کند. ما اغلب با چند رسته به‌طورهمزمان سرو کار خواهیم داشت. درنتیجه، اگر A و B اشیائی از رستهٔ $\mathcal{C}$ باشند، مجموعهٔ‌تمام‌ریخت‌هادر $\mathcal{C}$ از A به B را گاهی‌به‌جای $\hom(A,B)$ مثل قبل با $\hom_{\mathcal{C}}(A,B)$ نشان خواهیم داد.

تعریف ۱.۱ . فـرض‌کنیـم $\mathcal{C}$ و $\mathcal{D}$ رسته بـاشند. ***تابعگر همورد*** T از $\mathcal{C}$ به $\mathcal{D}$ (که با $T:\mathcal{C}\to\mathcal{D}$ نموده مـی‌شود) جفتی است از توابع (که هر دو با T نموده می‌شود)، یکی تابع شی که به هرشیء C از $\mathcal{C}$ شیء مانند $T(C)$ از $\mathcal{D}$ را نسبت مـی‌دهد و دیگری تابع ریخت که به هر ریخت $f:C\to C'$ از $\mathcal{C}$ ریختی مانند $T(f):T(C)\to T(C')$ از $\mathcal{D}$ را نسبت می‌دهد به‌طوری که (یک) به‌ازای هر ریخت همانی 1_C از $\mathcal{C}$ ، $T(1_C)=1_{T(C)}$ ؛ (دو) به‌ازای هـر دو ریخـت f,g از $\mathcal{C}$ که تـرکیب $g\circ f$ آنها تعـریف شـده بـاشـد، $T(g\circ f)=T(g)\circ T(f)$.

مثال. ***تابعگر همانی*** (همورد) $I_{\mathcal{C}}:\mathcal{C}\to\mathcal{C}$ هرشیء‌و هر ریخت از رستهٔ $\mathcal{C}$ را به خودش نسبت می‌دهد.

مثال. فرض‌کنیم R یک حلقـه بوده و A یک R ــ مدول چپ ثابتی باشد. به‌ازای هر

R ــ مدول C ، قرار می‌دهیم $T(C) = \mathrm{Hom}_R(A,C)$. به‌ازای هر همریختی $f : C \to C'$ از R ــ مدولها ، $T(f)$ رانگاشت‌القایی معمولی $f : \mathrm{Hom}_R(A,C) \to \mathrm{Hom}_R(A,C')$ می‌گیریم (ر.ک. چند تبصرهٔ بعد از قضیهٔ IV ۱.۴۰) . در این صورت ، T یک تابعگر هموردِ از رستهٔ R ــ مدولهای چپ به رستهٔ گروههای آبلی است .

مثال . به‌طور کلی ، فرض کنیم A شیٔ ثابتی در رستهٔ $\mathfrak{C}$ باشد . تابعگر هموردِ h_A از $\mathfrak{C}$ به رستهٔ $\mathfrak{S}$ از مجموعه‌ها را این‌طور تعریف می‌کنیم که به شیٔ C از $\mathfrak{C}$ مجموعهٔ $h_A(C) = \hom(A,C)$ مرکب از تمام‌ریختها در $\mathfrak{C}$ از A به C را نسبت می‌دهیم . اگر $f : C \to C'$ یک ریخت از $\mathfrak{C}$ باشد ، $h_A(f) : \hom(A,C) \to \hom(A,C')$ را تابعی می‌گیریم که با $(g \in \hom(A,C))$ $g \mapsto f \circ g$ داده می‌شود . تابعگر h_A ، که ذیلا" به تفصیل مورد بحث قرار می‌گیرد ، ***تابعگر هموردِ hom*** نام دارد .

مثال . فرض کنیم F تابعگر هموردِ زیر از رستهٔ مجموعه‌ها به رستهٔ مدولهای چپ روی حلقهٔ یکدار R باشد . به‌ازای هر مجموعهٔ X ، $F(X)$ ، R ــ مدول آزاد بر X است (ر.ک. چندتبصرهٔ بعدازقضیهٔ IV ۱.۲۰) . اگر $f : X \to X'$ یک تابع باشد ، $F(f) : F(X) \to F(X')$ را همریختی منحصر به فرد $\bar{f} : F(X) \to F(X')$ از مدولها می‌گیریم که $\bar{f}i = f$ ، که در آن i نگاشت شمول $X \to F(X)$ می‌باشد (قضیهٔ IV ۱.۲۰) .

مثال . فرض کنیم $\mathfrak{C}$ یک رستهٔ ملموس (تعریف I ۶.۷۰) نظیر رستهٔ R ــ مدولهای چپ یا گروهها یا حلقه‌ها ، باشد . ***تابعگر فراموشی*** (هموردِ) از $\mathfrak{C}$ به رستهٔ $\mathfrak{S}$ از مجموعه‌ها به هر شیٔ A مجموعهٔ زمینهٔ آن (که نیز با A نموده می‌شود) و به هر ریخت $f : A \to A'$ تابع $f : A \to A'$ را نسبت می‌دهد (ر.ک. تعریف I ۶.۷۰) .

تعریف ۲.۱ . فرض کنیم $\mathfrak{C}$ و $\mathfrak{D}$ رسته باشند . ***تابعگر پادوردِ*** S از $\mathfrak{C}$ به $\mathfrak{D}$ (که با $S : \mathfrak{C} \to \mathfrak{D}$ نموده می‌شود) جفتی از توابع است (که هر دو با S نموده می‌شوند) ، یکی تابع شیٔ که به هر شیٔ C از $\mathfrak{C}$ شیٔ مانند S(C) از $\mathfrak{D}$ رانسبت می‌دهد و دیگری تابع ریخت که به هر ریخت $f : C \to C'$ از $\mathfrak{C}$ ریخت

$$S(f) : S(C') \to S(C)$$

از $\mathfrak{D}$ را نسبت می‌دهد به‌طوری که

(یک) به‌ازای هر ریخت همانی 1_C از $\mathfrak{C}$ ، $S(1_C) = 1_{S(C)}$ ؛

(دو) به‌ازای هر دو ریخت f, g از $\mathfrak{C}$ که ترکیب $g \circ f$ آنها تعریف شده باشد ،

$S(g \circ f) = S(f) \circ S(g)$.

لذا ، تابع ریخت تابعگر پادورد $S : \mathfrak{C} \to \mathfrak{D}$ جهت ریختها را عوض می‌کند .

مثال . فرض کنیم R یک‌حلقه‌بوده و B یک R ــ مدول چپ ثابتی باشد . تابعگر پادورد S از رسته‌ٔ R ــ مدولهای‌چپ‌به‌رسته‌ٔ گروههای آبلی را با $S(C) = \mathrm{Hom}_R(C,B)$ به‌ازای هر R ــ مدول C تعریف می‌کنیم . هرگاه $f : C \to C'$ یک همریختی R ــ مدولها باشد ، آنگاه $S(f)$ نگاشت القایی $\bar{f} : \mathrm{Hom}_R(C',B) \to \mathrm{Hom}_R(C,B)$ می‌باشد (ر.ک. چند تبصرهٔ بعد از قضیهٔ IV ۱۰۴۰) .

مثال . به‌طور کلی ، فرض کنیم B شئ ثابتی در رستهٔ $\mathfrak{C}$ باشد . تابعگر پادورد h^B از $\mathfrak{C}$ به رستهٔ $\mathcal{S}$ از مجموعه‌ها را این‌طور تعریف می‌کنیم که به هر شئ C از $\mathfrak{C}$ مجموعهٔ $h^B(C) = \hom(C,B)$ مرکب از تمام ریختها در $\mathfrak{C}$ از C به B نسبت می‌دهیم . اگر $f : C \to C'$ یک ریخت از $\mathfrak{C}$ باشد ، تابع $h^B(f) : \hom(C',B) \to \hom(C,B)$ را با $g \mapsto g \circ f$ $(g \in \hom(C',B))$ تعریف می‌کنیم . تابعگر h^B را **تابعگر پادورد** $\hom\mathfrak{C}$ می‌نامند .

با استفاده از روش زیر می‌توان بررسی تابعگرهای پادورد را به بررسی تابعگرهای همورد تحویل کرد . هرگاه $\mathfrak{C}$ یک رسته باشد ، آنگاه رستهٔ **متقابل** (یا **دوگان**) $\mathfrak{C}$ ، که با $\mathfrak{C}^{\mathrm{op}}$ نموده می‌شود ، به صورت زیر تعریف می‌گردد . اشیاء $\mathfrak{C}^{\mathrm{op}}$ همان اشیاء $\mathfrak{C}$ اند . مجموعهٔ $\hom_{\mathfrak{C}^{\mathrm{op}}}(A,B)$ از ریختها در $\mathfrak{C}^{\mathrm{op}}$ از A به B مساوی مجموعهٔ $\hom_{\mathfrak{C}}(B,A)$ از ریختها در $\mathfrak{C}$ از B به A تعریف می‌شود . وقتی ریخت $f \in \hom_{\mathfrak{C}}(B,A)$ یک ریخت در $\hom_{\mathfrak{C}^{\mathrm{op}}}(A,B)$ درنظرگرفته‌شود ، آن را با f^{op} نشان می‌دهیم . ترکیب ریختها در $\mathfrak{C}^{\mathrm{op}}$ با

$$g^{\mathrm{op}} \circ f^{\mathrm{op}} = (f \circ g)^{\mathrm{op}}$$

تعریف می‌شود .

اگر $S : \mathfrak{C} \to \mathfrak{D}$ یک تابعگر پادورد باشد ، $S : \mathfrak{C}^{\mathrm{op}} \to \mathfrak{D}$ را تابعگر **همورد** منحصر به

فردی می‌گیریم که به‌ازای هر شیء A و ریخت f از $\mathcal{C}^{op}$ با

$$\bar{S}(f^{op}) = S(f) \quad \text{و} \quad \bar{S}(A) = S(A)$$

تعریف می‌شود. به عکس، به آسانی تحقیق می‌شود که هر تابعگر هموِرد بر $\mathcal{C}^{op}$ به همین نحو از یک تابعگر پادوِرد بر $\mathcal{C}$ ناشی می‌گردد.

به یاد آورید که هر حکم در رابطه با اشیاء و ریختهای یک رسته حکم دوگانی دارد که با عکس کردن جهت ریختها به دست می‌آید (ر.ک. ص ۸۴). به آسانی معلوم می‌شود که یک حکم در رستهٔ $\mathcal{C}$ درست است اگر و فقط اگر حکم دوگان آن در $\mathcal{C}^{op}$ درست باشد. درنتیجه، هر حکم مستلزم اشیاء، ریختها، و تابعگر پادوِرد S بر $\mathcal{C}$ درست است مشروط بر اینکه حکم دوگان آن برای تابعگر هموِرد $\bar{S}$ بر $\mathcal{C}^{op}$ درست باشد. به این دلیل بسیاری از نتایج آتی فقط برای تابعگرهای هموِرد ثابت می‌شوند، حالت پادوِرد به آسانی با دوگان سازی اثبات خواهد شد.

برای تعریف تابعگرهای چندمتغیره، شایسته است مفهوم **رستهٔ حاصلضربی** معرفی شود. اگر $\mathcal{C}$ و $\mathcal{D}$ رسته باشند، حاصلضرب آنها رستهٔ $\mathcal{C} \times \mathcal{D}$ است که اشیاء آن تمام جفتهای (C,D) اندکه C و D به‌ترتیب اشیاء $\mathcal{C}$ و $\mathcal{D}$ می‌باشند. ریخت $(C,D) \to (C',D')$ از $\mathcal{C} \times \mathcal{D}$ جفتی مانند (f,g) است، که در آن $f : C \to C'$ ریختی از $\mathcal{C}$ و $g : D \to D'$ ریختی از $\mathcal{D}$ است. ترکیب با $(f',g') \circ (f,g) = (f' \circ f, g' \circ g)$ تعریف می‌شود. اصول موضوع رسته‌ها به آسانی تحقیق می‌شوند. حاصلضرب بیش از دو رسته به همین نحو تعریف می‌گردد.

تابعگرهای چندمتغیره بر یک رستهٔ حاصلضربی مناسب تعریف می‌شوند. یک چنین تابعگر ممکن است نسبت به بعضی متغیرها هموِرد و نسبت به دیگران پادوِرد باشد. مثلاً، اگر $\mathcal{C},\mathcal{D},\mathcal{E}$ رسته باشند، تابعگر دومتغیرهٔ T (پادوِرد نسبت به متغیر اول و هموِرد نسبت به متغیر دوم) از $\mathcal{C} \times \mathcal{D}$ به $\mathcal{E}$ عبارت است از یک تابع شیء که به هر جفت از اشیاء (C,D) در $\mathcal{C} \times \mathcal{D}$ شیء $T(C,D)$ از $\mathcal{E}$ را نسبت می‌دهد، و یک تابع ریخت که به هر جفت ریخت مانند $f : C \to C'$, $g : D \to D'$ از $\mathcal{C} \times \mathcal{D}$ ریخت

$$T(f,g) : T(C',D) \to T(C,D')$$

از $\mathcal{E}$ را نسبت می‌دهد تحت شرایط زیر:

(یک) به‌ازای هر (C,D) در $\mathcal{C} \times \mathcal{D}$، $T(1_C,1_D) = 1_{T(C,D)}$؛

(دو) هرگاه ترکیبات $f' \circ f$, $g' \circ g$ به ترتیب در $\mathcal{C}$ و $\mathcal{D}$ تعریف شده باشند، آنگاه

$T(f' \circ f, g' \circ g) = T(f,g') \circ T(f',g)$. شرط دوم ایجاب می‌کند که به‌ازای هر شیء ثابت C از $\mathcal{C}$ ، تابع شیء $T(C,-)$ و تابع ریخت $T(1_C,-)$ یک تابعگر همورد $\mathcal{D} \to \mathcal{E}$ را تشکیل می‌دهند . به همین نحو ، به‌ازای هر شیء ثابت D از $\mathcal{D}$ ، $T(-,D)$ و $T(-,1_D)$ یک تابعگر پادورد مانند $\mathcal{C} \to \mathcal{E}$ را تشکیل خواهند داد .

مثال . $\mathrm{Hom}_R(-,-)$ یک تابعگر دو متغیره است ، پادورد نسبت به اولی و همورد نسبت به دومی ، از رستهٔ R ــ مدولهای چپ $\mathfrak{M}$ [1] به رستهٔ گروههای آبلی .

مثال . به‌طورکلی ، فرض کنیم $\mathcal{C}$ یک رسته‌باشد . تابعگری درنظر می‌گیریم که به هرجفت (A,B) از اشیاء $\mathcal{C}$ مجموعهٔ $\hom_{\mathcal{C}}(A,B)$ و به‌هرجفت از ریختهای $f : A \to A', g : B \to B'$ تابع

$$\hom(f,g) : \hom_{\mathcal{C}}(A',B) \to \hom_{\mathcal{C}}(A,B')$$

را نسبت می‌دهد که با $h \mapsto g \circ h \circ f$ تعریف می‌شود . $\hom_{\mathcal{C}}(-,-)$ یک تابعگر دومتغیره از $\mathcal{C}$ به رستهٔ $\mathcal{S}$ از مجموعه‌ها است ، پادوردنسبت به متغیر اول و همورد نسبت به متغیر دوم . توجه کنید که به‌ازای شیء ثابت A ، $\hom_{\mathcal{C}}(A,-)$ چیزی جز تابعگر همورد hom ، یعنی h_A نیست و $h_A(g) = \hom(1_A,g)$. به همین نحو ، به‌ازای B ی ثابت ، $\hom_{\mathcal{C}}(-,B)$ تابعگر پادورد hom ، یعنی h^B است و $h^B(f) = \hom(f,1_B)$.

مثال . فرض کنیم K یک حلقهٔ یکدار باشد . در این صورت ، تابعگر

$$T(A_1, \ldots, A_n) = A_1 \otimes_K \cdots \otimes_K A_n$$
$$T(f_1, \ldots, f_n) = f_1 \otimes \cdots \otimes f_n$$

یک تابعگر n متغیرهٔ همورد از رستهٔ K ــ مدولها به خودش است .

هرگاه $T_1 : \mathcal{C} \to \mathcal{D}$ و $T_2 : \mathcal{D} \to \mathcal{E}$ تابعگر باشند ، آنگاه **ترکیب** آنها (که با T_2T_1 نموده می‌شود) تابعگری از $\mathcal{C}$ به $\mathcal{E}$ است که توابع شیء و ریخت آن عبارتند از

---

۱ . *به بیان دقیق ، $\mathrm{Hom}_R(-,-)$ یک تابعگر بر $\mathfrak{M} \times \mathfrak{M}$ است ، ولی این سوءاستعمال از زبان رایج بوده و ابهامی ایجاد نمی‌کند .*

$$C \to T_2(T_1(C));$$
$$f \to T_2(T_1(f)).$$

T_2T_1 همورد است اگر T_1 و T_2 هر دو همورد یا هر دو پادورد باشند. T_2T_1 پادورد است اگر یکی از T_i ها همورد و دیگری پادورد باشد.

تعریف ۳.۱. فرض کنیم $\mathcal{C}$ و $\mathcal{D}$ رسته‌بوده‌و $S:\mathcal{C}\to\mathcal{D}$, $T:\mathcal{C}\to\mathcal{D}$ تابعگرهایی همورد باشند. ***تبدیل طبیعی*** $\alpha:S\to T$ تابعی‌است‌که‌به‌هرشی C از $\mathcal{C}$ ریخت $\alpha_C:S(C)\to T(C)$ از $\mathcal{D}$ را چنان نسبت می‌دهد که به‌ازای هر ریخت $f:C\to C'$ از $\mathcal{C}$ ، نمودار

$$\begin{array}{ccc} S(C) & \xrightarrow{\alpha_C} & T(C) \\ \downarrow{\scriptstyle S(f)} & & \downarrow{\scriptstyle T(f)} \\ S(C') & \xrightarrow[\alpha_{C'}]{} & T(C') \end{array}$$

در $\mathcal{D}$ تعویضپذیر است. هرگاه α_C یک تعادل به‌ازای هر C در $\mathcal{C}$ باشد، آنگاه α یک **یکریختی طبیعی** (یا **تعادل طبیعی**) از تابعگرهای S و T می‌باشد.

تبدیل طبیعی [یکریختی] $\beta:S\to T$ از تابعگرهای **پادورد** $S,T:\mathcal{C}\to\mathcal{D}$ به همین نحو تعریف می‌شود جز آنکه نمودار تعویضپذیر مطلوب به‌ازای هر ریخت $f:C\to C'$ از $\mathcal{C}$ عبارت است از

$$\begin{array}{ccc} S(C) & \xrightarrow{\beta_C} & T(C) \\ \uparrow{\scriptstyle S(f)} & & \uparrow{\scriptstyle T(f)} \\ S(C') & \xrightarrow[\beta_{C'}]{} & T(C'). \end{array}$$

چند تبصره. ترکیب دو تبدیل طبیعی بوضوح یک تبدیل طبیعی است. تبدیلات طبیعی تابعگرهای چندمتغیره به طرز مشابهی تعریف می‌شوند.

مثال. هرگاه $T:\mathcal{C}\to\mathcal{C}$ یک تابعگرباشد، آنگاه انتساب $C\mapsto 1_{T(C)}$ یک یکریختی طبیعی مانند $I_T:T\to T$ را تعریف می‌کند که **یکریختی طبیعی همانی** نامیده می‌شود.

مثال. فرض کنیم $\mathfrak{M}$ رستهٔ مدولهای چپ روی حلقهٔ R بوده و $T:\mathfrak{M}\to\mathfrak{M}$ تابعگر

دوگان مضاعف باشدکه به‌هر مدول A مدول دوگان مضاعف آن $A^{**} = \mathrm{Hom}_R(\mathrm{Hom}_R(A,R),R)$ را نسبت می‌دهد. به‌ازای هر مدول A ، $\theta_A : A \to A^{**}$ را همریختی قضیهٔ IV ۱۲.۴۰ می‌گیریم. در ایـن صورت، انتساب $A \mapsto \theta_A$ یک تبدیل طبیعـی از تابعگر همانی $I_{\mathfrak{M}}$ به تابعگر T تعریف می‌کند (تمرین IV ۹.۴۰) . هرگاه رستهٔ $\mathfrak{M}$ با رستهٔ $\mathfrak{U}$ مرکب از تمام فضاهای‌برداری‌چپ با بعد متناهی روی حلقهٔ بخشی T عوض شـده و T را تابعگری چون $\mathfrak{U} \to \mathfrak{U}$ درنظربگیریم ،آنگاه ،بنابرقضیهٔ IV ۱۲.۴۰ (سه) ، انتساب $A \mapsto \theta_A$ $(A \in \mathfrak{U})$ یک **یکریختی** طبیعی از $I_{\mathfrak{U}}$ به T را تعریف می‌کند. همچنین ، ر.ک. تمرین ۵ .

تبدیلات طبیعی‌بارها با لباس مبدل در رسته‌هایی خاص ظاهر می‌شوند. مثلا" ، در رستهٔ R ــ مدولها (و نیز گروهها ، حلقه‌ها ، و غیره) ، می‌توان بدون ذکر تابعگر گفت که یک همـریختی طبیعی اسـت. این معمولا" بیان خلاصه‌ای است به معنی زیر: دو تابعگر (نسبتا" واضح) و یک تبدیل طبیعی بین آنها وجود دارد.

مثال. هرگاه B یک مـدول چـپ یکانی روی حلقهٔ یکدار R باشد ، آنگاه یک یکریختی طبیعی از مدولها مانند $\alpha_B : R \otimes_R B \cong B$ وجود دارد (ر.ک. قضیـهٔ IV ۷.۵۰) . به آسانی تحقیق می‌شود که به‌ازای هر همریختی مدولها مانند $f : B \to C$ ، نمودار

$$\begin{array}{ccc} R \otimes_R B & \xrightarrow{\alpha_B} & B \\ {\scriptstyle 1_R \otimes f}\downarrow & & \downarrow{\scriptstyle f} \\ R \otimes_R C & \xrightarrow[\alpha_C]{} & C \end{array}$$

تعویض‌پذیراست .لذا ،عبارت "یکریختی طبیعی" یعنی انتساب $B \mapsto \alpha_B$ یکریختی طبیعی $\alpha : T \to I_{\mathfrak{M}}$ را تعریف مـی‌کند ، کـه در آن $\mathfrak{M}$ رستـهٔ R ــ مدولهای‌چپ یکانی بوده و $T : \mathfrak{M} \to \mathfrak{M}$ با $B \mapsto R \otimes_R B$ و $f \mapsto 1_R \otimes f$ داده شده‌اند.

مثال. هرگاه A,B,C مدولهای‌چپ‌روی حلقهٔ R باشند ، آنگاه یکریختی گروههای آبلی

$$\phi : \mathrm{Hom}_R(A \oplus B, C) \cong \mathrm{Hom}_R(A,C) \oplus \mathrm{Hom}_R(B,C)$$

در قضیهٔ IV ۷.۴۰ طبیعی است. در اینجا می‌توان واژهٔ "طبیعی" را با ثابت گرفتن دو متغیر ، مثـلا" A و C ، و توجه به اینکه به‌ازای هر همریختی $f : B \to B'$ از مدولها

نمودار

$$\begin{array}{ccc} \mathrm{Hom}_R(A \oplus B', C) & \xrightarrow{\phi} & \mathrm{Hom}_R(A,C) \oplus \mathrm{Hom}_R(B',C) \\ \downarrow{\scriptstyle \mathrm{Hom}(1_A \oplus f, 1_C)} & & \downarrow{\scriptstyle \mathrm{Hom}(1_A, 1_C) \oplus \mathrm{Hom}(f, 1_C)} \\ \mathrm{Hom}_R(A \oplus B, C) & \xrightarrow{\phi} & \mathrm{Hom}_R(A,C) \oplus \mathrm{Hom}_R(B,C) \end{array}$$

تعویضپذیر است، تعبیر کرد، که در این نمودار $1_A \oplus f : A \oplus B \to A \oplus B'$ با $(a,b) \mapsto (a, f(b))$ داده می‌شود. لذا، ϕ یک یکریختی طبیعی تابعگرهای پادورد S و T را تعریف می‌کند، که

$$S(B) = \mathrm{Hom}_R(A \oplus B, C) \quad \text{و} \quad T(B) = \mathrm{Hom}_R(A,C) \oplus \mathrm{Hom}_R(B,C) .$$

گویند یکریختی ϕ **در** $\mathbf{B}$ **طبیعی** است. استدلالی مشابه نشان می‌دهد که ϕ نسبت به A و C نیز طبیعی است.

مثالهای دیگر در تمرین ۴ ذکر شده‌اند.

تعریف ۴.۱. فرض کنیم T یک‌تابعگر هموردا زرستهٔ $\mathcal{C}$ به‌رستهٔ $\mathcal{S}$ از مجموعه‌ها باشد. گوییم T یک ***تابعگر نمایشپذیر*** است اگر شیئ‌ٔ مانند A در $\mathcal{C}$ و یک یکریختی طبیعی مانند α از تابعگر هموردا hom یعنی $\mathbf{h_A} = hom_{\mathcal{C}}(\mathrm{A}, -)$ به‌تابعگر T وجود داشته باشند. جفت (A, α) یک ***نمایش*** T نام دارد و گوییم T به‌وسیلهٔ شیئ‌ٔ A نمایش داده شده است.

به همین نحو، گوییم تابعگر پادورد $\mathrm{S} : \mathcal{C} \to \mathcal{S}$ ***نمایشپذیر*** است اگر شبیئ‌ٔ مانند B از $\mathcal{C}$ و یک یکریختی طبیعی مانند $\beta : \mathbf{h^B} \to \mathrm{S}$ وجود داشته باشند، که در آن $\mathbf{h^B} = \mathrm{hom}_{\mathcal{C}}(-, \mathrm{B})$. گوییم (B, β) یک ***نمایش*** S می‌باشد.

مثال. فرض کنیم A و B مدولهایی یکانی روی حلقهٔ تعویضپذیر و یکدار K بوده و، به‌ازای هر K ــ مدول C، $T(C)$ را مجموعهٔ تمام نگاشتهای K ــ دوخطی $A \times B \to C$ می‌گیریم. اگر $f : C \to C'$ یک همریختی K ــ مدولها باشد، $T(f) : T(C) \to T(C')$ را تابعی می‌گیریم که نگاشت دوخطی $g : A \times B \to C$ را به‌نگاشت دوخطی $fg : A \times B \to C'$ می‌برد. در این صورت، T یک تابعگر هموردا از رستهٔ $\mathfrak{M}$ از K ــ مدولها به رستهٔ $\mathcal{S}$ از مجموعه‌ها می‌باشد. حکم می‌کنیم که T به وسیلهٔ K ــ مدول $A \otimes_K B$ نمایش داده می‌شود. برای مشاهدهٔ این امر، به‌ازای هر K ــ مدول C، تابع

$$\alpha_C : \mathrm{Hom}_K(A \otimes_K B, C) \to T(C)$$

را با $\alpha_C(f) = fi$ تعریف می‌کنیم ،که در آن $i : A \times B \to A \otimes_K B$ نگاشت دوخطی کانونی است (ر.ک. ص ۳۲۹) . اما $\alpha_C(f) : A \times B \to C$ به‌ازای هر $f \in \mathrm{Hom}_K(A \otimes_K B, C)$ بوضوح دوخطی است. بنابر قضیهٔ IV ۶.۵۰ ، هرنگاشت دوخطی $g : A \times B \to C$ به شکل $\bar{g}i$ است ، که در آن $\bar{g} : A \otimes_K B \to C$ همریختی K ــ مدولهای منحصربه‌فرداست . بنابراین ، α_C یک بیژکسیون مجموعه‌هاست (یعنی ، یک تعادل در رستهٔ $\mathcal{S}$) . به آسانی تحقیق می‌شود که انتساب $C \mapsto \alpha_C$ یک یکریختی طبیعی از $h_{A \otimes_K B}$ به T تعریف می‌کند ؛ درنتیجه ، $(A \otimes_K B, \alpha)$ یک نمایش T می‌باشد . این امر که $A \otimes_K B$ یک شیٔ عمومی در یک رستهٔ مناسب است تصادفی نیست (قضیهٔ IV ۶.۵۰) . حال نشان می‌دهیم که حکم مشابهی برای هر تابعگر نمایشپذیر درست است .

فرض کنیم (A, α) نمایش تابعگرهمورد $T : \mathcal{C} \to \mathcal{S}$ باشد .همچنین ، $\mathcal{C}_T$ رسته‌ای باشد که اشیاء آن تمام جفتهایی به صورت (C, s) باشند ، که در آن C یک شیٔ $\mathcal{C}$ بوده و $s \in T(C)$. یک ریخت در $\mathcal{C}_T$ از (C, s) به (D, t) ریختی مانند $f : C \to D$ از $\mathcal{C}$ تعریف می‌شود که $T(f)(s) = t \in T(D)$. توجه کنید که f یک تعادل در $\mathcal{C}_T$ است اگر و فقط اگر f یک تعادل در $\mathcal{C}$ باشد . یک شیٔ عمومی در رستهٔ $\mathcal{C}_T$ (ر.ک. تعریف I ۹.۷۰) یک **عنصر عمومی** تابعگر T نامیده می‌شود .

مثال . در مثال بعد از تعریف ۴.۱ ، این امر که $(A \otimes_K B, \alpha)$ نمایشی از تابعگر $T : \mathfrak{M} \to \mathcal{S}$ است بوضوح ایجاب می‌کند که به‌ازای هر K ــ مدول C و نگاشت دوخطی $f : A \times B \to C$ (یعنی ، به‌ازای هر جفت (C, f) که $f \in T(C)$) ، یک همریختی منحصر به فرد از K ــ مدولها مانند $\bar{f} : A \otimes_K B \to C$ وجوددارد به‌طوری که $\bar{f}i = f$ (یعنی ، طوری که $T(\bar{f})(i) = f$ که در آن $i = \alpha_{A \otimes_K B}(1_{A \otimes_K B}) \in T(A \otimes_K B)$) . درنتیجه ، جفت $(A \otimes_K B, i) = (A \otimes_K B, \alpha_{A \otimes_K B}(1_{A \otimes_K B}))$ یک شیٔ عمومی در رستهٔ $\mathfrak{M}_T$ است ؛ یعنی ، یک عنصر عمومی T می‌باشد .

حال ، با مثال پیش به‌عنوان انگیزه ، نشان می‌دهیم که نمایشهای تابعگر $T : \mathcal{C} \to \mathcal{S}$ اساساً " با عناصر عمومی T معادلند . در این راه به لم زیر نیاز داریم

لم ۵۰۱ . *فرض کنیم* $T : \mathcal{C} \to \mathcal{S}$ *یک تابعگرهمورد از رستهٔ* $\mathcal{C}$ *به رستهٔ* $\mathcal{S}$ *از مجموعه‌ها بوده و* A *شیئ از* $\mathcal{C}$ *باشد .*

(یک) هرگاه $\alpha : h_A \to T$ *یک تبدیل طبیعی از تابعگر همورد* hom ، h_A *به* T *بوده و* $u = \alpha_A(1_A) \in T(A)$ ، *آنگاه ، به‌ازای هر شیئ* C *از* $\mathcal{C}$ *و* $g \in hom_{\mathcal{C}}(A,C)$ ،

$$\alpha_C(g) = T(g)(u).$$

(دو) هرگاه $u \in T(A)$ *و به‌ازای هرشیئ* C *از* $\mathcal{C}$ ، $\beta_C : hom_{\mathcal{C}}(A,C) \to T(C)$ *نگاشتی باشد که با* $g \mapsto T(g)(u)$ *تعریف شده است ، آنگاه* $\beta : h_A \to T$ *یک تبدیل طبیعی است به‌طوری که* $\beta_A(1_A) = u$.

برهان . (یک) فرض کنیم C شیئ از $\mathcal{C}$ بوده و $g \in \hom_{\mathcal{C}}(A,C)$. طبق فرض، نمودار

$$\begin{array}{ccc} h_A(A) = \hom_{\mathcal{C}}(A,A) & \xrightarrow{\alpha_A} & T(A) \\ {\scriptstyle h_A(g)}\downarrow & & \downarrow{\scriptstyle T(g)} \\ h_A(C) = \hom_{\mathcal{C}}(A,C) & \xrightarrow[\alpha_C]{} & T(C) \end{array}$$

تعویضپذیر است . درنتیجه ،

$$\begin{aligned} \alpha_C(g) &= \alpha_C(g \circ 1_A) = \alpha_C[h_A(g)(1_A)] \\ &= [\alpha_C h_A(g)]\,(1_A) = (T(g)\alpha_A)(1_A) = T(g)[\alpha_A(1_A)] \\ &= T(g)(u). \end{aligned}$$

(دو) باید نشان دهیم که به‌ازای هر ریخت $k : B \to C$ از $\mathcal{C}$ ، نمودار

$$\begin{array}{ccc} h_A(B) = \hom_{\mathcal{C}}(A,B) & \xrightarrow{\beta_B} & T(B) \\ {\scriptstyle h_A(k)}\downarrow & & \downarrow{\scriptstyle T(k)} \\ h_A(C) = \hom_{\mathcal{C}}(A,C) & \xrightarrow[\beta_C]{} & T(C) \end{array}$$

تعویضپذیر است . این مطلب فورا " نتیجه می‌شود ، زیرا به‌ازای هر $f \in \hom_{\mathcal{C}}(A,B)$ ،

$$\begin{aligned} [\beta_C h_A(k)](f) &= \beta_C(k \circ f) = T(k \circ f)(u) = [T(k)T(f)](u) \\ &= T(k)[T(f)(u)] = T(k)[\beta_B(f)] \\ &= [T(k)\beta_B](f). \end{aligned}$$

بنابراین ، β یک تبدیل طبیعی است . بالاخره ،

$$\beta_A(1_A) = T(1_A)(u) = 1_{T(A)}(u) = u.$$

قضیهٔ ۶۰۱ . *فرض کنیم* $T : \mathcal{C} \to \mathcal{S}$ *یک تابعگر هموردا زرستهٔ* $\mathcal{C}$ *به‌رستهٔ* $\mathcal{S}$ *از مجموعه‌ها باشد . تناظر یک به یکی بین ردهٔ* X *مرکب از تمام نمایشهای* T *و ردهٔ* Y *مرکب از تمام عناصر عمومی* T *وجود دارد که با* $(A,\alpha) \mapsto (A,\alpha_A(1_A))$ *تعریف می‌شود .*

تبصره . چون $\alpha_A : \hom_{\mathcal{C}}(A,A) \to T(A)$ ، $\alpha_A(1_A)$ عنصری از $T(A)$ است .

برهان ۶۰۱ . فرض کنیم (A,α) نمایشی از T بوده و $\alpha_A(1_A) = u \in T(A)$. همچنین ، (B,s) شیئ‌ٔ از $\mathcal{C}_T$ باشد . طبق فرض ، $\alpha_B : h_A(B) = \hom_{\mathcal{C}}(A,B) \to T(B)$ یک بیژکسیون است ، که از آنجا ، به‌ازای ریخت منحصر به فردی چون $f : A \to B$ ، $s = \alpha_B(f)$. بنابر لم ۵۰۱ ، داریم $T(f)(u) = \alpha_B(f) = s$. بنابراین ، f یک ریخت در $\mathcal{C}_T$ از (A,u) به (B,s) می‌باشد . هرگاه g ریخت دیگری در $\mathcal{C}_T$ از (A,u) به (B,s) باشد ، آنگاه $g \in \hom_{\mathcal{C}}(A,B)$ و $T(g)(u) = s$ ، درنتیجه ، بنابر لم ۵۰۱ $\alpha_B(g) = T(g)(u) = s = \alpha_B(f)$ چون α_B بیژکسیون است ، $f = g$. بنابراین ، f ریخت منحصر به فرد در $\mathcal{C}_T$ از (A,u) به (B,s) است ؛ درنتیجه ، (A,u) در $\mathcal{C}_T$ عمومی می‌باشد . لذا ، (A,u) یک عنصر عمومی T خواهد بود .

به عکس ، فرض کنیم (A,u) یک عنصر عمومی T باشد . همچنین ، $\beta : h_A \to T$ تبدیل طبیعی لم ۵۰۱ (دو) باشد به‌طوری که به‌ازای هر شیئ‌ٔ C از $\mathcal{C}$ ، $\beta_C : \hom_{\mathcal{C}}(A,C) \to T(C)$ با $\beta_C(f) = T(f)(u)$ تعریف می‌شود . هرگاه $s \in T(C)$ ، آنگاه (C,s) در $\mathcal{C}_T$ می‌باشد . چون (A,u) در $\mathcal{C}_T$ عمومی است ، $f \in \hom_{\mathcal{C}}(A,C)$ ی وجود دارد به‌طوری‌که $s = T(f)(u) = \beta_C(f)$. بنابراین ، β_C سورژکتیو می‌باشد . هرگاه $\beta_C(f_1) = \beta_C(f_2)$ ، آنگاه

$$T(f_1)(u) = \beta_C(f_1) = \beta_C(f_2) = T(f_2)(u)$$

که از آنجا f_1 و f_2 هر دو ریختهایی در $\mathcal{C}_T$ از (A,u) به

$$(C,T(f_1)(u)) = (C,T(f_2)(u))$$

می‌باشند . درنتیجه ، بنابر عمومی بودن ، $f_1 = f_2$. بنابراین ، هر β_C انژکتیو و لذا بیژکسیون می‌باشد (تعادل در $\mathcal{S}$) . لذا ، β یک یکریختی طبیعی است ؛ درنتیجه ، (A,β) یک نمایش T خواهد بود .

برای اتمام برهان، با استفاده از لم ۵.۱ تحقیق کنید که $\psi\phi = 1_X$ و $\phi\psi = 1_Y$، که در آن $\phi : X \to Y$ با $(A,\alpha) \mapsto (A,\alpha_A(1_A))$ و $\psi : Y \to X$ با $(A,u) \mapsto (A,\beta)$ تعریف می‌شود (β مثل بند پیش است). بنابراین، ϕ یک بیژکسیون می‌باشد.

نتیجهٔ ۷.۱. *فرض کنیم $T : \mathcal{C} \to \mathcal{S}$ یک تابعگر هموردا از رستهٔ $\mathcal{C}$ به رستهٔ $\mathcal{S}$ از مجموعه‌ها باشد. هرگاه (A,α) و (B,β) نمایشهایی از T باشند، آنگاه تعادل منحصر به فردی مانند $f : A \to B$ وجود دارد به‌طوری‌که نمودار زیر به‌ازای هر شیٔ C از $\mathcal{C}$ تعویضپذیر است:*

$$\begin{array}{ccc} h_B(C) = \hom_{\mathcal{C}}(B,C) & & \\ \Big\downarrow{\scriptstyle \hom(f,1_C)} & \searrow^{\beta_C} & \\ & & T(C) \\ & \nearrow_{\alpha_C} & \\ h_A(C) = \hom_{\mathcal{C}}(A,C) & & \end{array}$$

برهان. فرض کنیم $u = \alpha_A(1_A)$ و $v = \beta_B(1_B)$. بنابرلم ۶.۱، (A,u) و (B,v) عناصری عمومی‌از T اند؛ درنتیجه، بنابرلم I ۱۰.۷۰، تعادل منحصر به فردی چون $f : A \to B$ در $\mathcal{C}$ وجود دارد به‌طوری که $T(f)(u) = v$. لم ۵.۱ (یک) ایجاب می‌کند که به‌ازای هر شیٔ C از $\mathcal{C}$ و $g \in \hom_{\mathcal{C}}(B,C)$،

$$\begin{aligned} [\alpha_C \hom(f,1_C)](g) &= \alpha_C(g \circ f) = T(g \circ f)(u) \\ &= [T(g)T(f)](u) = T(g)[T(f)(u)] = T(g)(v) \\ &= \beta_C(g). \end{aligned}$$

درنتیجه، نمودار مطلوب تعویضپذیر است. به علاوه، هرگاه $f_1 : A \to B$ نیز نمودار را تعویضپذیر سازد، آنگاه، به‌ازای $C = B$ و $g = 1_B$،

$$T(f_1)(u) = \alpha_B(f_1) = \alpha_B(1_B \circ f_1) = \alpha_B[\hom(f_1,1_B)(1_B)] = \beta_B(1_B) = v.$$

بنابراین، طبق یکتایی، $f_1 = f$.

نتیجهٔ ۸.۱ (یوندا[1]). *فرض کنیم $T : \mathcal{C} \to \mathcal{S}$ یک تابعگر هموردا از رستهٔ $\mathcal{C}$ به رستهٔ $\mathcal{S}$ از مجموعه‌ها بوده و A شیٔ از $\mathcal{C}$ باشد. دراین صورت، تناظر یک به یکی بین مجموعهٔ*

---

1. *Yoneda*

$T(A)$ و مجموعهٔ $Nat(h_A,T)$ مرکب‌از تمام تبدیلات طبیعی از تابعگر هموردِ hom ، h_A به تابعگر T وجود دارد . این بیژکسیون نسبت به A و T طبیعی می‌باشد .

طرح برهان . تابع $\psi = \psi_A : \mathrm{Nat}(h_A,T) \to T(A)$ را با

$$\alpha \mapsto \alpha_A(1_A) \in T(A)$$

و تابع $\phi : T(A) \to \mathrm{Nat}(h_A,T)$ را با

$$u \mapsto \beta$$

تعریف می‌کنیم ، که در آن β از لم ۵.۱ (دو) به دست می‌آید . تحقیق کنید که $\phi\psi$ و $\psi\phi$ نگاشتهای همانی مربوطه‌اند . بنابراین ، ψ_A بیژکسیون است .

حکم طبیعی بودن نتیجه بدین معنی است که نمودارهای

$$\begin{array}{ccc} \mathrm{Nat}(h_A,T) & \xrightarrow{\psi_A} & T(A) \\ {\scriptstyle N^*(f)}\downarrow & & \downarrow{\scriptstyle T(f)} \\ \mathrm{Nat}(h_B,T) & \xrightarrow[\psi_B]{} & T(B) \end{array} \quad ,$$

$$\begin{array}{ccc} \mathrm{Nat}(h_A,T) & \xrightarrow{\psi_A} & T(A) \\ {\scriptstyle N_*(\alpha)}\downarrow & & \downarrow{\scriptstyle \alpha_A} \\ \mathrm{Nat}(h_A,S) & \xrightarrow[\psi_A]{} & S(A) \end{array}$$

تعویضپذیرند ،که‌درآنها $f : A \to B$ ریختی از $\mathcal{C}$ و $\alpha : T \to S$ تبدیلی طبیعی از تابعگرها بوده و $N^*(f), N_*(\alpha)$ به‌صورت‌زیرتعریف‌می‌شوند . به‌ازای‌هرشیٔ C از $\mathcal{C}$ و $\beta \in \mathrm{Nat}(h_A,T)$ ،

$$N^*(f)(\beta)_C : h_B(C) = \mathrm{hom}_{\mathcal{C}}(B,C) \to T(C)$$

با $g \mapsto \beta_C(g \circ f)$ تعریف‌می‌شود . نگاشت $N_*(\alpha) : \mathrm{Nat}(h_A,T) \to \mathrm{Nat}(h_A,S)$ با $\beta \mapsto \alpha\beta$ داده می‌شود .

تابعگر نمایشپذیر یک تابعگر یک متغیره است که به‌طور طبیعی با تابعگر هموردِ (یا پادورد) hom یکریخت است . اما ، به‌ازای رستهٔ مفروض $\mathcal{D}$ ، $\mathrm{hom}_{\mathcal{D}}(-,-)$ تابعگری از دو متغیر است . حال شرایطی را بررسی می‌کنیم که تابعگر دو متغیرهٔ T تحت آنها با $\mathrm{hom}_{\mathcal{D}}(-,-)$ به‌طور طبیعی یکریخت باشد .

به وضعیت به نوعی کلیتر زیر می‌پردازیم . فرض کنیم $\mathcal{C}$ و $\mathcal{D}$ دو رسته بوده و

$T : \mathcal{C} \times \mathcal{D} \to \mathcal{S}$ تابعگری باشدکه نسبت به متغیر اول پادورد و نسبت به متغیر دوم همورد است. هرگاه $S : \mathcal{C} \to \mathcal{D}$ یک‌تابعگرهمورد باشد، آنگاه به آسانی تحقیق می‌شود که انتسابهای $(C,D) \mapsto \hom_{\mathcal{D}}(S(C),D)$ و $(f,g) \mapsto \hom_{\mathcal{D}}(S(f),g)$ یک تابعگر مانند $\mathcal{C} \times \mathcal{D} \to \mathcal{S}$ تعریف می‌کنند که نسبت به متغیر اول پادورد و نسبت به متغیر دوم همورد است.

قضیهٔ ۹۰۱. *فرض کنیم $\mathcal{C}$ و $\mathcal{D}$ رسته بوده و T تابعگری از رستهٔ حاصلضربی $\mathcal{C} \times \mathcal{D}$ به رستهٔ $\mathcal{S}$ از مجموعه‌ها باشدکه نسبت به متغیر اول پادورد و نسبت به متغیر دوم همورد است به‌طوری که، به‌ازای هر شیٔ C از $\mathcal{C}$، تابعگرهمورد $T(C,-) : \mathcal{D} \to \mathcal{S}$ دارای نمایش (A_C,α^C) می‌باشد. در این صورت، تابعگر همورد منحصر به فردی مانند $S : \mathcal{C} \to \mathcal{D}$ وجود دارد به‌طوری که $S(C) = A_C$ و یک یکـریختی‌طبیعی از $hom_{\mathcal{D}}(S(-),-)$ به T وجود دارد که با*

$$\alpha^C{}_D : hom_{\mathcal{D}}(S(C),D) \to T(C,D)$$

تعریف می‌شود.

تبصره در باب نمادگذاری. به‌ازای‌هرشیٔ C از $\mathcal{C}$، شیٔ A_C در $\mathcal{D}$ و α^C یک‌یکریختی طبیعی از $\hom_{\mathcal{D}}(A_C,-)$ به $T(C,-)$ است. لذا، به‌ازای هر D در $\mathcal{D}$، یک تعادل مانند $\alpha^C{}_D : \hom_{\mathcal{D}}(A_C,D) \to T(C,D)$ وجود خواهد داشت.

برهان ۹۰۱. تابع شیٔ‌تابعگر S به‌ازای‌هرشیٔ C از $\mathcal{C}$ با $S(C) = A_C$ تعریف می‌شود. تابع ریخت S به صورت زیر تعریف می‌شود. به‌ازای هر شیٔ C از $\mathcal{C}$،

$$\alpha^C{}_{AC} : \hom_{\mathcal{D}}(A_C,A_C) \to T(C,A_C) \quad \text{و} \quad u_C = \alpha^C{}_{AC}(1_{AC}) \in T(C,A_C) .$$

بنابر قضیهٔ ۶۰۱، (A_C,u_C) عنصری عمـومی از تابعگر $T(C,-)$ است. اگر $f : C \to C'$ یک ریخت از $\mathcal{C}$ باشد، قـرار مـی‌دهیم $v = T(f,1_{AC'})(u_{C'}) \in T(C,A_{C'})$. بنابر عمـومی بودن (A_C,u_C) در $\mathcal{D}$، ریخت منحصر به فردی مانند $\bar{f} : A_C \to A_{C'}$ در $\mathcal{D}$ وجود دارد به‌طوری‌که

$$T(1_C,\bar{f})(u_C) = v = T(f,1_{AC'})(u_{C'}).$$

$S(f)$ را ریخت $\bar{f}$ تعریف می‌کنیم.

واضح است که $S(1_C) = 1_{AC} = 1_{S(C)}$. هرگاه $C \xrightarrow{f} C' \xrightarrow{g} C''$ ریختهایی از $\mathcal{C}$ باشند، آنگاه، طبق تعریف، $S(g)$ ریخت منحصر به فردی چون $\bar{g} : A_{C'} \to A_{C''}$ است به‌طوری‌که

$$T(1_{C'},\bar{g})(u_{C'}) = T(g,1_{AC''})(u_{C''}).$$

به همین نحو، $S(g \circ f)$ ریخت منحصر به فردی مانند $\bar{h} : A_C \to A_{C''}$ است به‌طوری که

$$T(1_C,\bar{h})(u_C) = T(g \circ f,1_{AC''})(u_{C''}).$$

درنتیجه، $S(g) \circ S(f) = \bar{g} \circ \bar{f}$ ریختی مانند $A_C \to A_{C''}$ است به‌طوری‌که

$$\begin{aligned} T(1_C,\bar{g} \circ \bar{f})(u_C) &= T(1_C,\bar{g})T(1_C,\bar{f})(u_C) = T(1_C,\bar{g})T(f,1_{AC'})(u_{C'}) \\ &= T(f,\bar{g})(u_{C'}) = T(f,1_{AC''})T(1_{C'},\bar{g})(u_{C'}) \\ &= T(f,1_{AC''})T(g,1_{AC''})(u_{C''}) = T(g \circ f,1_{AC''})(u_{C''}) \\ &= T(1_C,\bar{h})(u_C). \end{aligned}$$

بنابراین، طبق خاصیت یکتایی اشیاء عمومی در $\mathfrak{D}_{T(C,-)}$، باید داشته باشیم

$$S(g) \circ S(f) = \bar{g} \circ \bar{f} = \bar{h} = S(g \circ f).$$

لذا، $S : \mathfrak{C} \to \mathfrak{D}$ یک تابعگر هممورد است.

برای آنکه نشان دهیم $\alpha : \hom_{\mathfrak{D}}(S(-),-) \to T$ یکریختی طبیعی است، کافی است ثابت کنیم به‌ازای ریختهای $f : C \to C'$ در $\mathfrak{C}$ و $g : D \to D'$ در $\mathfrak{D}$، نمودار

$$\begin{array}{ccc} \hom_{\mathfrak{D}}(A_{C'},D) & \xrightarrow{\alpha^{C'}{}_D} & T(C',D) \\ \downarrow{\scriptstyle \hom(S(f),1_D)} & & \downarrow{\scriptstyle T(f,1_D)} \\ \hom_{\mathfrak{D}}(A_C,D) & \xrightarrow{\alpha^{C}{}_D} & T(C,D) \\ \downarrow{\scriptstyle \hom(1_{AC},g)} & & \downarrow{\scriptstyle T(1_C,g)} \\ \hom_{\mathfrak{D}}(A_C,D') & \xrightarrow[\alpha^{C}{}_{D'}]{} & T(C,D') \end{array}$$

تعویضپذیر است. مربع پایینی تعویضپذیر است زیرا، طبق فرض، به‌ازای C ی ثابت،

$$\alpha^C : \hom_{\mathfrak{D}}(A_C,-) \to T(C,-)$$

یک یکریختی طبیعی می‌باشد. برای مربع بالایی، فرض کنیم $k \in \hom_{\mathfrak{D}}(A_{C'},D)$. در این صورت، طبق لم ۵.۱ (یک)،

$$\begin{aligned} T(f,1_D)\alpha^{C'}{}_D(k) &= T(f,1_D)T(1_{C'},k)(u_{C'}) = T(f,k)(u_{C'}) \\ &= T(1_C,k)T(f,1_{AC'})(u_{C'}) = T(1_C,k)T(1_C,\bar{f})(u_C) \\ &= T(1_C,k \circ \bar{f})(u_C) = T(1_C,k \circ S(f))(u_C) \\ &= \alpha^{C}{}_{D'}(k \circ S(f)) \\ &= \alpha^{C}{}_{D'}\hom(S(f),1_D)(k). \end{aligned}$$

تمرینات

تذکر. در این تمرینات $\mathcal{S}$ رستهٔ مجموعه‌ها و توابع، $\mathcal{R}$ رستهٔ حلقه‌ها و همریختیهای

حلقه‌ها، R یک حلقه، $\mathfrak{M}$ رستهٔ R ــ مدولهای چپ و همریختیهای R ــ مدولها، $\mathfrak{S}$ رستهٔ گروهها و همریختیهای گروهها می‌باشد.

۱. تابعگرها را به صورت زیر بسازید.

(آ) تابعگر هموردِ $\mathfrak{S} \to \mathfrak{S}$ که به هر گروه مجموعهٔ تمام زیرگروههای آن را نسبت می‌دهد.

(ب) تابعگر هموردِ $\mathfrak{R} \to \mathfrak{R}$ که به هر حلقهٔ N حلقهٔ چندجمله‌ایهای $N[x]$ را نسبت می‌دهد.

(پ) تابعگر $\mathfrak{M} \times \mathfrak{M} \to \mathfrak{M}$ هموردِ نسبت به هر دو متغیر به‌طوری که

$$(A,B) \mapsto A \oplus B.$$

(ت) تابعگر هموردِ $\mathfrak{S} \to \mathfrak{S}$ که به هر گروه G زیرگروه تعویضگر G' را نسبت می‌دهد (تعریف II ۷۰۷۰).

۲. (آ) اگر $T : \mathfrak{C} \to \mathfrak{D}$ یک تابعگر هموردِ باشد، $\operatorname{Im} T$ را مرکب از اشیاء $\{T(C) \mid C \in \mathfrak{C}\}$ و ریختهای

$$\{T(f) : T(C) \to T(C') \mid f : C \to C' \text{ یک ریخت در } \mathfrak{C} \text{ است}\}$$

بگیرید. سپس نشان دهید که $\operatorname{Im} T$ لزوماً یک رسته نیست.

(ب) هرگاه تابع شیٔ T انژکتیو باشد، آنگاه $\operatorname{Im} T$ یک رسته است.

۳. (آ) هرگاه $S : \mathfrak{C} \to \mathfrak{D}$ یک تابعگر باشد، فرض کنید $\sigma(S) = 1$ اگر S هموردِ و -1 اگر S پادوردِ باشد. اگر $T : \mathfrak{D} \to \mathfrak{E}$ تابعگردیگری باشد، نشان دهید که TS تابعگری از $\mathfrak{C}$ به $\mathfrak{E}$ است که پراش آن با $\sigma(TS) = \sigma(T)\sigma(S)$ داده می‌شود.

(ب) قسمت (آ) را به هر تعداد متناهی تابعگر مانند

$$S_1 : \mathfrak{C}_1 \to \mathfrak{C}_2, S_2 : \mathfrak{C}_2 \to \mathfrak{C}_3, \ldots, S_n : \mathfrak{C}_n \to \mathfrak{C}_{n+1}$$

تعمیم دهید.

۴. (آ) هرگاه A,B,C مجموعه باشند، آنگاه بیژکسیونهایی طبیعی مانند $A \times B \to B \times A$ و $(A \times B) \times C \to A \times (B \times C)$ وجود دارند.

(ب) ثابت کنید یکریختیهای قضایای IV ۴۰۹۰، IV ۸۰۵۰، IV ۹۰۵۰، و IV ۱۰۰۵۰ همه طبیعی‌اند.

۵. فرض کنید $\mathfrak{V}$ رسته‌ای باشد که اشیاء آن همهٔ فضاهای برداری با بعد متناهی روی میدان F (با مشخص مخالف 2 و 3) و ریختهایش همهٔ یکریختیهای فضاهای

برداری بـاشند . فضای دوگان V^* از فضای برداری چپ V را به عنوان یک فضای برداری چپ درنظر بگیرید (ر.ک. تبصرهٔ بعد از حکم VII ۱۰.۱۰) .

(آ) هرگاه $\phi : V \to V_1$ یک یکـریختی فضـاهای برداری باشد (ریختی از $\mathcal{U}$) ، آنگاه نگاشت دوگان $\phi^* : V_1^* \to V^*$ نیز چنین است (ر.ک. قضیهٔ IV ۱۰.۴۰) . از اینرو ، $\phi^{-1} : V^* \to V_1^*$ نیز ریختی از $\mathcal{U}$ می‌باشد .

(ب) $D : \mathcal{U} \to \mathcal{U}$ یک تـابعگر هموردِ است ، که در آن $D(V) = V^*$ و $D(\phi) = \phi^{-1}$.

(پ) بـه‌ازای هـر V در $\mathcal{U}$ ، پـایـهٔ $\{x_1, \ldots, x_n\}$ را اختیار کرده و فرض کنید $\{f_{x_1}, \ldots, f_{x_n}\}$ پایهٔ دوگان V^* باشد (قضیهٔ IV ۱۱.۴۰) . در این صورت ، نگاشت $\alpha_V : V \to V^*$ تعریف شده با $x_i \mapsto f_{x_i}$ یکریختی است . بنابراین ، $\alpha_V : V \cong D(V)$.

(ت) یکریختی α_V طبیعی نیست ؛ یعنی ، انتساب $V \mapsto \alpha_V$ یک یکریختی طبیعی از تابعگر همانی $I_{\mathcal{U}}$ به D نیست . [**راهنمایی .** فضای یک بعدی با پایهٔ $\{x\}$ را درنظر گرفته و فرض کنید $\phi(x) = cx$ که در آن $c \neq 0, \pm 1_F$.]

۶ . (آ) فرض کنید $S : \mathcal{C} \to \mathcal{D}$ و $T : \mathcal{C} \to \mathcal{D}$ تابعگرهای هموردِ بوده و $\alpha : S \to T$ یک یکریختی طبیعی باشد . در این صورت ، یکریختی طبیعیی مانند $\beta : T \to S$ وجود دارد به‌طوری که $\beta\alpha = I_S$ و $\alpha\beta = I_T$ ، که در آن $I_S : S \to S$ یکریختی طبیعی همانی اسـت و همیـن‌طـور در مـورد I_T . [**راهنمایی .** بـه‌ازای هـر C از $\mathcal{C}$ ، $\alpha_C : S(C) \to T(C)$ یک تعادل است ؛ و در نتیجه ، ریخت معکوسی چون $\beta_C : T(C) \to S(C)$ دارد .]

(ب) قسمت (آ) را به تابعگرهای چندمتغیره تعمیم دهید .

۷ . تابعگرهای نمایشپذیر هموردِ از $\mathcal{S}$ به $\mathcal{S}$ نگاشتهای سورژکتیو را حفظ می‌کنند .

۸ . (آ) تابعگر فراموشی $\mathcal{M} \to \mathcal{S}$ (ر.ک. مثال پیش از تعریف ۲۰.۱) نمایشپذیر است .

(ب) تابعگر فراموشی $\mathcal{G} \to \mathcal{S}$ نمایشپذیر است .

۹ . (آ) فـرض کنیـد $P : \mathcal{S} \to \mathcal{S}$ تابعگری بـاشد که به هر مجموعهٔ X مجموعهٔ توان (مجموعهٔ تمام زیرمجموعه‌های) آن $P(X)$ را نسبت دهد و به هر تابع $f : A \to B$ نگاشت $P(f) : P(B) \to P(A)$ را نسبـت دهـد کـه زیرمجموعهٔ X از B را به روی $f^{-1}(X) \subset A$ می‌برد . دراین صورت ، P یک تابعگر پادوردِ نمایشپذیر است .

(ب) فـرض کنیـد تابع شیٔ $Q : \mathcal{S} \to \mathcal{S}$ با $Q(A) = P(A)$ تعریف شـده باشد . اگر $f : A \to B$ ، $Q(f) : Q(A) \to Q(B)$ را با $X \mapsto f(X)$ تعریف نمایید . در این صورت ،

Q یک تابعگر هموردست. آیا Q نمایشپذیر است؟

۱۰. فرض کنید (A,α) و (B,β) نمایشهایی از تابعگرهای هموردی $S:\mathcal{C}\to\mathcal{S}$ و $T:\mathcal{C}\to\mathcal{S}$ باشند. هرگاه $\tau:S\to T$ تبدیلی طبیعی باشد، آنگاه ریخت منحصر به فردی مانند $f:A\to A$ در $\mathcal{C}$ وجوددارد به‌طوری‌که نمودارزیربه‌ازای هر شیء C از $\mathcal{C}$ تعویضپذیر است:

$$\begin{array}{ccc} \hom_{\mathcal{C}}(A,C) & \xrightarrow{\alpha_C} & S(C) \\ {\scriptstyle \hom(f,1_C)}\downarrow & & \downarrow{\scriptstyle \tau_C} \\ \hom_{\mathcal{C}}(B,C) & \xrightarrow[\beta_C]{} & T(C) \end{array}$$

۲ تابعگرهای الحاقی

جفتهای الحاقی از تابعگرهاتعریف و مورد بحث قرار گرفتند. با آنکه آنها در بسیاری از شاخه‌های ریاضی ظاهرمی‌شوند، توصیف‌صوری آنها تا حدودی اخیرا" صورت یافته است.

فرض کنیم $S:\mathcal{C}\to\mathcal{D}$ و $T:\mathcal{D}\to\mathcal{C}$ تابعگرهای‌هموردی‌باشند. همانطور که در بحث پیش ازقضیهٔ ۹.۱ دیدیم، انتسابهای $(C,D)\mapsto \hom_{\mathcal{D}}(S(C),D)$ و $(f,g)\mapsto \hom_{\mathcal{D}}(S(f),g)$ تابعگری مانند $\mathcal{C}\times\mathcal{D}\to\mathcal{S}$ تعریف می‌کنندکه‌نسبت به متغیر اول پادورد و نسبت به متغیر دوم هموردست. این تابعگر را با $\hom_{\mathcal{D}}(S(-),-)$ نشان می‌دهیم. به همین نحو، تابعگر با $\hom_{\mathcal{C}}(-,T(-)):\mathcal{C}\times\mathcal{D}\to\mathcal{S}$

$$(f,g)\mapsto \hom_{\mathcal{C}}(f,T(g)) \quad و \quad (C,D)\mapsto \hom_{\mathcal{C}}(C,T(D))$$

تعریف شده است.

تعریف ۱۰۲. فرض کنیم $T:\mathcal{D}\to\mathcal{C}$ و $S:\mathcal{C}\to\mathcal{D}$ تابعگرهای هموردی باشند. گوییم S یک *الحاق چپ* T است (یا T یک *الحاق راست* S است یا (S,T) یک *جفت الحاقی* است) اگر یک یکریختی طبیعی از تابعگر $hom_{\mathcal{D}}(S(-),-)$ به تابعگر $hom_{\mathcal{C}}(-,T(-))$ موجود باشد.

لذا، اگر S یک الحاق چپ T باشد، به‌ازای هر C از $\mathcal{C}$ و D از $\mathcal{D}$ یک بیژکسیون مانند

$$\alpha_{C,D} : \hom_{\mathfrak{D}}(S(C),D) \to \hom_{\mathfrak{C}}(C,T(D))$$

وجود دارد که نسبت به C و D طبیعی است. نظریهٔ تابعگرهای الحاقی اول بار از مثال زیر نشأت گرفته است.

مثال. فرض کنیم R, S حلقه بوده و $A_R, {}_RB_S, C_S$ (دو) مدولهای مربوطه باشند. بنابر قضیهٔ IV ۱۰.۵۰، یک یکریختی از گروههای آبلی مانند

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$$

وجود دارد، که به آسانی می‌توان نشان داد که نسبت به A و C (و نیز نسبت به B) طبیعی است. توجه کنید که، بنابر قضیهٔ IV ۵.۵۰ (سه)، $A \otimes_R B$ یک S ــ مدول راست است و، بنابرتمرین IV ۴.۴۰ (پ)، $\mathrm{Hom}_S(B,C)$ یک R ــ مدول راست می‌باشد. فرض کنیم B یک R-S دو مدول ثابت باشد. همچنین، $\mathfrak{C}$ رستهٔ R ــ مدولهای راست و $\mathfrak{D}$ رستهٔ S ــ مدولهای راست باشد؛ درنتیجه، $\hom_{\mathfrak{C}}(X,Y) = \mathrm{Hom}_R(X,Y)$ و $\hom_{\mathfrak{D}}(U,V) = \mathrm{Hom}_S(U,V)$. در این صورت، یکریختی بالا صرفا" می‌گویدکه تابعگر $-\otimes_R B$ از $\mathfrak{C}$ به $\mathfrak{D}$ یک الحاق چپ تابعگر $\hom_S(B,-)$ از $\mathfrak{D}$ به $\mathfrak{C}$ می‌باشد.

مثال. فرض کنیم R حلقه‌ای یکدار بوده و $\mathfrak{M}$ رستهٔ R ــ مدولهای چپ یکانی باشد. همچنین، $T : \mathfrak{M} \to \mathfrak{S}$ تابعگر فراموشی باشد که به هر مدول مجموعهٔ زمینه‌اش را نسبت می‌دهد. در این صورت، به‌ازای هر مجموعهٔ X و مدول A، $\hom_{\mathfrak{S}}(X,T(A))$ چیزی جز مجموعهٔ تمام توابع $X \to A$ نیست. فرض کنیم $F : \mathfrak{S} \to \mathfrak{M}$ تابعگری باشد که به هر X، R ــ مدول آزاد $F(X)$ بر مجموعهٔ X را نسبت می‌دهد (ر.ک. ص ۲۸۴). فرض کنیم $i_X : X \to F(X)$ نگاشت کانونی باشد. به آسانی معلوم می‌شود که، به‌ازای هر مجموعهٔ X و مدول A، نگاشت

$$\alpha_{X,A} : \mathrm{Hom}_R(F(X),A) \to \hom_{\mathfrak{S}}(X,T(A))$$

تعریف شده با $g \mapsto gi_X$ نسبت به X و A طبیعی است. چون $F(X)$ بر X آزاد است، $\alpha_{X,A}$ انژکتیو می‌باشد (قضیهٔ IV ۱.۲۰ (چهار)). به علاوه، هر تابع $f : X \to T(A)$ به شکل $f = \bar{f} i_X$ است، که در آن $\bar{f} : F(X) \to A$ یک همریختی منحصربه فرد است (قضیهٔ IV ۱.۲۰ (چهار)). درنتیجه، $\alpha_{X,A}$ سورژکتیو و درنتیجه بیژکسیون می‌باشد. بنابراین، F یک الحاق چپ T می‌باشد.

مثالهای دیگر در تمرینات ذکر شده‌اند.

بین جفتهای الحاقی از تابعگرها و تابعگرهای نمایشپذیر رابطهٔ نزدیکی وجود دارد.

حکم ۲.۲. *تابعگر هموردِ $T:\mathcal{D}\to\mathcal{C}$ الحاق چپ دارد اگر و فقط اگر به‌ازای هر شیء C در $\mathcal{C}$، تابعگر $hom_{\mathcal{C}}(C,T(-)):\mathcal{D}\to\mathcal{S}$ نمایشپذیر باشد.*

برهان. هرگاه $S:\mathcal{C}\to\mathcal{D}$ یک الحاق چپ T باشد، آنگاه، به‌ازای هر شیء C از $\mathcal{C}$ و D از $\mathcal{D}$، یک بیژکسیون مانند

$$\alpha_{C,D}:\hom_{\mathcal{D}}(S(C),D)\to\hom_{\mathcal{C}}(C,T(D))$$

وجود دارد که نسبت به C و D طبیعی است. لذا، به‌ازای C ی ثابتی، $(S(C),\alpha_{C,-})$ یک نمایش تابعگر $\hom_{\mathcal{C}}(C,T(-))$ می‌باشد.

به عکس، فرض کنیم به‌ازای هر C، A_C شیئی از $\mathcal{D}$ باشد که $\hom_{\mathcal{C}}(C,T(-))$ را نمایش می‌دهد. بنابر قضیهٔ ۹.۱، تابعگر هموردی مانند $S:\mathcal{C}\to\mathcal{D}$ وجود دارد به‌طوری که $S(C)=A_C$ و یک یکریختی طبیعی از تابعگرها مانند

$$\hom_{\mathcal{D}}(S(-),-)\to\hom_{\mathcal{C}}(-,T(-))$$

موجود است. بنابراین، S یک الحاق چپ T می‌باشد.

نتیجهٔ ۳.۲. *تابعگر هموردِ $T:\mathcal{D}\to\mathcal{C}$ دارای الحاق چپ است اگر و فقط اگر به‌ازای هر شیء C از $\mathcal{C}$ یک شیء مانند $S(C)$ از $\mathcal{D}$ و یک ریخت مانند $u_C:C\to T(S(C))$ موجود باشد به‌طوری که $(S(C),u_C)$ یک عنصر عمومی از تابعگر $hom_{\mathcal{C}}(C,T(-)):\mathcal{D}\to\mathcal{S}$ باشد.*

برهان. تمرین؛ ر.ک. قضیهٔ ۶.۱.

نتیجهٔ ۴.۲. *هر دو الحاق چپ تابعگر هموردِ $T:\mathcal{D}\to\mathcal{C}$ به‌طور طبیعی یکریخت‌اند.*

برهان. هرگاه $S_1:\mathcal{C}\to\mathcal{D}$ و $S_2:\mathcal{C}\to\mathcal{D}$ الحاقهای چپ T باشند، آنگاه یکریختیهای طبیعی زیر وجود دارند:

$$\alpha : \hom_{\mathfrak{D}}(S_1(-),-) \to \hom_{\mathfrak{C}}(-,T(-)),$$
$$\beta : \hom_{\mathfrak{D}}(S_2(-),-) \to \hom_{\mathfrak{C}}(-,T(-)).$$

به‌ازای هر شیء C از $\mathfrak{C}$ ، اشیاء $S_1(C)$ و $S_2(C)$ هردو ،طبق‌قسمت‌اول‌برهان حکم ۲.۲ ، تابعگر $\hom_{\mathfrak{C}}(C,T(-))$ را نمایش‌می‌دهند .بنابراین ، طبق نتیجهٔ ۷.۱ ، به‌ازای هر شیء C از $\mathfrak{C}$ یک تعادل مانند $f_C : S_1(C) \to S_2(C)$ وجوددارد .کافی‌است نشان دهیم که f_C در C طبیعی است؛ یعنی ،به‌ازای ریخت داده شدهٔ $g : C \to C'$ از $\mathfrak{C}$ ، باید ثابت کنیم‌که

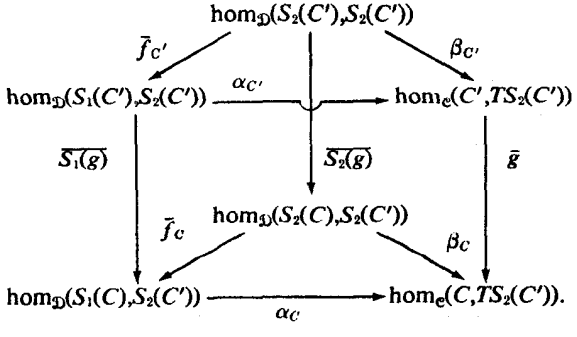
$$\begin{array}{ccc} S_1(C) & \xrightarrow{f_C} & S_2(C) \\ {\scriptstyle S_1(g)}\downarrow & & \downarrow{\scriptstyle S_2(g)} \\ S_1(C') & \xrightarrow[f_{C'}]{} & S_2(C') \end{array}$$

تعویضپذیر است . کافی است ثابت کنیم که

$$\begin{array}{ccc} \hom_{\mathfrak{D}}(S_1(C'),S_2(C')) & \xleftarrow{\hom(f_{C'},1)} & \hom_{\mathfrak{D}}(S_2(C'),S_2(C')) \\ {\scriptstyle \hom(S_1(g),1)}\downarrow & & \downarrow{\scriptstyle \hom(S_2(g),1)} \\ \hom_{\mathfrak{D}}(S_1(C),S_2(C')) & \xleftarrow[\hom(f_C,1)]{} & \hom_{\mathfrak{D}}(S_2(C),S_2(C')) \end{array}$$

تعویضپذیر است (که در آن $1 = 1_{S_2(C')}$) . زیرا نقش $1_{S_2(C')}$ در یک جهت $S_2(g) \circ f_C$ و در جهت دیگر $f_{C'} \circ S_1(g)$ می‌باشد .

نمودار سه‌بعدی زیر را درنظر می‌گیریم (که در آن $\alpha_X = \alpha_{X,S_2(C')}$ ، $1 = 1_{S_2(C')}$ و، برای سادگی ، نگاشت القایی $\hom(k,1)$ با $\bar{k}$ نموده شده است) :



باید ثابت کنیم که مستطیل عقبی چپ تعویضپذیر است . مثلثهای بالا و پایین طبق

نتیجهٔ ۷۰۱ تعویضپذیرند. مستطیلهای جلـوی و عقبی راست تعویضپذیرند، زیرا α و β طبیعی می‌باشند؛ درنتیجه،

$$\alpha_C\overline{S_1(g)}\,\bar{f}_{C'} = \bar{g}\alpha_{C'}\,\bar{f}_{C'} = \bar{g}\beta_{C'} = \beta_C\overline{S_2(g)} = \alpha_C\,\bar{f}_C\overline{S_2(g)}.$$

چون طبق فرض $\alpha_C = \alpha_{C,S_2(C')}$ انژکتیو است، باید داشته باشیم $\overline{S_1(g)}\,\bar{f}_{C'} = \bar{f}_C\overline{S_2(g)}$. بنابراین، مستطیل عقبی چپ تعویضپذیر می‌باشد.

تمرینات

تذکر. $\mathcal{S}$ رستهٔ مجموعه‌هاست.

۱. هرگاه $T:\mathcal{C}\to\mathcal{S}$ یک تابعگر هموِرد باشد که الحاق چپ دارد، آنگاه T نمایشپذیر است.

۲. فرض کنید $\mathcal{C}$ یک رستهٔ ملموس بوده و $T:\mathcal{C}\to\mathcal{S}$ تابعگر فراموشی باشد. هرگاه T دارای الحاق چپ $F:\mathcal{S}\to\mathcal{C}$ باشد، آنگاه F یک ***تابعگر آزاد شیء*** و $F(X)\,(X\in\mathcal{S})$ یک ***Fـآزاد شیء*** بر X نامیده می‌شود.

(آ) رستهٔ گروهها دارای تابعگر آزاد شیء است.

(ب) رستهٔ حلقه‌های تعـویضپذیر یکدار و همریختیهای حافظ‌واحد دارای تابعگر آزاد شیء است. [اگر X متناهی باشد، $F(X)$ را با استفاده از تمرین III ۱۱۰۵۰ تعریف کنید.]

۳. فرض کنید X مجموعه‌ای ثـابت بوده و تابعگر $S:\mathcal{S}\to\mathcal{S}$ را با $Y\mapsto X\times Y$ تعریف کنید. در این صورت تابعگر S یک الحاق چپ تابعگر هموِرد $h_X = \hom_{\mathcal{S}}(X,-)$ است.

۴. فرض کنید $\mathcal{G}$ رستهٔ گروهها، $\mathcal{A}$ رستهٔ گروههای آبلی، $\mathcal{F}$ رستهٔ میدانها، $\mathcal{D}$ رستهٔ دامنه‌های صحیـح، $\mathfrak{M}$ رستـهٔ K ـ مدولهای چپ یکانی، و $\mathcal{B}$ رستهٔ K-K دو مدولهای یـکانی باشد (K,R حلقه و یکدار هستند). در هر یک از حالات زیر، فرض کنید T تابعگر فراموشی مقتضی باشد (مثلا "، $T:\mathcal{F}\to\mathcal{D}$ هر میدان را، که‌به عنوان دامنهٔ صحیح درنظر گرفته شده، به خودش می‌برد). نشان دهید که (S,T) — یک جفت الحاقی می‌باشد.

(آ) $T:\mathcal{A}\to\mathcal{G}$, $S:\mathcal{G}\to\mathcal{A}$، که درآن $S(G) = G/G'$ و G' زیرگروه تعویضـگر G است (تعریف II ۷۰۷۰).

(ب) $T:\mathcal{F}\to\mathcal{D}, S:\mathcal{D}\to\mathcal{F}$ ، که در آن $S(D)$ میدان خارج‌قسمتها است (بخش III . ۴).

(پ) $T:\mathfrak{M}\to\mathfrak{A}, S:\mathfrak{A}\to\mathfrak{M}$ ، که در آن $S(A)=K\otimes_{\mathbf{Z}}A$ (ر.ک. قضیهٔ IV ۵۰۵۰).

(ت) $T:\mathfrak{B}\to\mathfrak{M}, S:\mathfrak{M}\to\mathfrak{B}$ ، که در آن $S(M)=M\otimes_{\mathbf{Z}}R$.

۳ ریختها

بخش مهم نظریهٔ مقدماتی رسته‌ها تعمیم هرچه بیشتر مفاهیم از رسته‌های مشهور (مثلا "، مجموعه‌ها یا مدولها) به رسته‌هایی دلخواه است. در این بخش مفاهیم تکریختی، برووریختی، هسته، و هم‌هستهٔ ریختها را به رسته‌های (بیش و کم) دلخواه تعمیم می‌دهیم.

نمادگذاری. از حالا به بعد معمولا " ترکیب دو ریخت از یک رسته را به جای $g\circ f$ قبلی با gf نشان می‌دهیم.

ابتدا به یاد می‌آوریم که ریخت $f:C\to D$ در یک رسته یک تعادل است اگر و فقط اگر ریختی مانند $g:D\to C$ موجود باشد به‌طوری که $gf=1_C$ و $fg=1_D$. این تعریف صرفا " انعکاس این امر است که هر همریختی در رستهٔ گروهها (یا حلقه‌ها، یا مدولها، و غیره) یک یکریختی است اگر و فقط اگر معکوس دوطرفه داشته باشد (ر.ک. قضیهٔ I ۳۰۲۰). به همین نحو، می‌توان مفاهیم تکریختی و برووریختی را به صورت زیر به رسته‌های دلخواه تعمیم داد.

تعریف ۱۰۳. ریخت $f:C\to D$ از رستهٔ $\mathcal{C}$ **تکین** (یا **تکریختی**) است اگر به‌ازای جمیع اشیاء B و ریختهای $g,h\in hom(B,C)$ ،

$$fh=fg \quad\Rightarrow\quad h=g.$$

ریخت f **برویی** (یا **برووریختی**) است اگر به‌ازای جمیع اشیاء E و ریختهای $k,t\in hom(D,E)$،

$$kf=tf \quad\Rightarrow\quad k=t.$$

مثال. یک ریخت در رستهٔ مجموعه‌ها تکین [برویی] است اگر و فقط اگر انژکتیو [سورژکتیو] باشد (تمرین ۱).

چند مثال. فرض کنیم $\mathcal{C}$ یکی از رسته‌های زیر باشد: گروهها، حلقه‌ها، مدولهای چپ

روی یک حلقه. هرگاه $f : C \to D$ و $g,h : B \to C$ همریختی (یعنی، ریختهایی در $\mathfrak{C}$) باشند، آنگاه، بنابر تمرین IV ۲.۱.۰ (آ)، $fh = fg$ ایجاب می‌کند که $h = g$ اگر و فقط اگر f یک همریختی انژکتیو (یعنی، یک تکریختی به معنی معمول) باشد.[1] لذا، تعریف رسته‌ای تکریختی با تعریف قبلی در این رسته‌های آشنا سازگار است.

چند مثال. تمرین IV. ۲.۱ (بـ) نشان می‌دهد که ریخت f در رستهٔ مدولهای چپ روی حلقهٔ R برویی است اگر و فقط اگر f یک همریختی سورژکتیو باشد (یعنی، یک برووریختی به معنی معمولی). همین امر در رستهٔ گروهها درست است ولی برهانش مشکلتر می‌باشد (تمرین ۲). لذا، تعریف رسته‌ای برووریختی با تعریف قبلی‌اش دراین دو رسته سازگار است.

چند مثال. در رستهٔ حلقه‌ها به آسانی معلوم می‌شود که هر همریختی سورژکتیو برویی است. اما، هرگاه $f,g : \mathbf{Q} \to R$ همریختی حلقه‌ها باشند به‌طوری‌که $f \mid \mathbf{Z} = g \mid \mathbf{Z}$، آنگاه، بنابر تمرین III ۱.۸.۱۰، $f = g$. درنتیجه، نگاشت شمول $\mathbf{Z} \to \mathbf{Q}$ در رستهٔ حلقه‌ها برویی است. اما این نگاشت بوضوح سورژکتیو نیست.

مثال. نگاشت کانونی $\pi : \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ در رستهٔ گروههای آبلی بخشپذیر (ص ۳۰۴) و همریختیهای گروهها تکین است ولی انـژکتیو نیست. برای مشاهدهٔ این امر، فرض کنیم $g,h : A \to \mathbf{Q}$ همـریختی بـوده و A بخشپذیر باشد و $\pi g = \pi h$. هرگاه $g \neq h$، آنگاه $a \in A, r,s \in \mathbf{Z}$ $(s \neq \pm 1)$ وجوددارند به‌طوری‌که $g(a) - h(a) = r/s \neq 0$. طبق فرض، به‌ازای $b \in A$ ای، $rb = a$، درنتیجه، $r(g(b) - h(b)) = g(a) - h(a) = r(1/s)$، که‌ازآنجا $g(b) - h(b) = 1/s$. بنابراین، $\pi(1/s) = \pi g(b) - \pi h(b) = \pi(g(b) - h(b)) = 0$. لذا، $1/s \in \operatorname{Ker} \pi = \mathbf{Z}$. که تناقض است زیرا $s \neq \pm 1$. بنابراین، $g = h$؛ و درنتیجه، π تکین است.

حکم ۲.۳. فرض کنیم $f : B \to C$ و $g : C \to D$ ریختهایی از رستهٔ $\mathfrak{C}$ باشند.
(یک) gf تکین $\Rightarrow$ f تکین؛ (دو) f تکین $\Rightarrow$ gf تکین؛

---

۱. تمرین مذکورفقط در رابطه با مدولهاست، ولی همین استدلال برای گروهها و حلقه‌ها نیز معتبر است.

(سه) gf بروییِ ⇒ f و g بروییِ؛ (چهار) g بروییِ ⇒ gf بروییِ؛
(پنج) f تکین و بروییِ ⇒ f یک تعادل.

برهان. تمرین.

تبصره. دو مثال پیش ازحکم ۲.۳ نشان می‌دهند که عکس قسمت (پنج) درست نیست.

شیءِ 0 در رستهٔ $\mathcal{C}$ را یک شیءِ صفر گوییم اگر 0 در $\mathcal{C}$ عمومی و هم عمومی‌باشد (ر.ک. تعریف I' ۹.۷۰). لذا، به‌ازای هرشیءِ C از $\mathcal{C}$، ریخت منحصر به فردی چون $C \to 0$ و ریخت منحصر به فردی مانند $0 \to C$ وجود دارد.

مثال. مدول صفر یک شیءِ صفر در رستهٔ مدولهای چپ روی یک حلقه است؛ به همین ترتیب، در مورد گروهها و حلقه‌ها. رستهٔ مجموعه‌ها دارای اشیاءِ صفر نیست.

حکم ۳.۳. فرض‌کنیم $\mathcal{C}$ یک رسته بوده و C شیئی از آن باشد.
(یک) هر دو شیءِ صفر از $\mathcal{C}$ باهم معادلند.
(دو) هرگاه 0 یک شیءِ صفر باشد، آنگاه ریخت منحصر به فرد $C \to 0$ تکین و ریخت منحصر به فرد $0 \to C$ بروییِ است.

طرح برهان. (یک) قضیهٔ I ۱۰.۷۰. (دو) هرگاه $0_C \circ f = 0_C \circ g$ که در آن $0_C : 0 \to C$، آنگاه، بنابرهم عمومی بودن 0، $f = g$. بنابراین، 0_C تکین است.

حکم ۴.۳. فرض‌کنیم $\mathcal{C}$ رسته‌ای باشد که دارای شیءِ صفر 0 است. در این صورت، به‌ازای هر جفت C,D از اشیاءِ $\mathcal{C}$، یک ریخت منحصر به فرد مانند $0_{C,D} : C \to D$ وجود دارد به‌طوری که به‌ازای جمیع ریختهای

$$0_{C,D} \circ g = 0_{B,D} \quad f \circ 0_{C,D} = 0_{C,E}, \quad f \in hom(D,E), \quad g \in hom(B,C)$$

تبصره. $0_{C,D}$ یک ریخت صفر نامیده می‌شود.

برهان ۴.۳ (یکتایی) هرگاه $\{0'_{C,D}\}$ و $\{0_{C,D}\}$ دو خانواده از ریختها با خواص مذکور باشند، آنگاه به‌ازای هر جفت C,D

$$0_{C,D} = 0'_{D,D}0_{C,D} = 0'_{C,D}.$$

(وجود) به‌ازای هرشیء A از $\mathcal{C}$، فرض‌کنیم $\iota_A : 0 \to A$ و $\pi_A : A \to 0$ ریختهای منحصر به فردی باشند. بنابر عمومی بودن، به‌ازای هر $f \in \hom(D,E)$ داریم $f\iota_D = \iota_E : 0 \to E$. بنابر هم‌عمومی بودن، به‌ازای هر $g \in \hom(B,C)$، $\pi_C g = \pi_B : B \to 0$. $0_{C,D}$ را ترکیب $C \xrightarrow{\pi_C} 0 \xrightarrow{\iota_D} D$ تعریف می‌کنیم. در این صورت، به‌ازای $f \in \hom(D,E)$،

$$f \circ 0_{C,D} = f\iota_D\pi_C = \iota_E\pi_C = 0_{C,E}$$

و به همین نحو در مورد حالت دیگر.

آخرین گام درتعمیم خواص ریختها در رسته‌های آشنا به ریختها در رسته‌های دلخواه ارائهٔ تعاریف معقولی از هسته‌ها و هم‌هسته‌های ریختها می‌باشد. مطلب را در محدودهٔ کلیتری آغاز می‌کنیم.

تعریف ۵.۳ . فرض کنیم $f : C \to D$ و $g : C \to D$ ریختهایی از رستهٔ $\mathcal{C}$ باشند. یک *هستهٔ تفاضلی* (یا *مساوی‌ساز*) برای جفت (f,g) ریختی است مانند $i : B \to C$ به‌طوری‌که

(یک) $fi = gi$ ؛

(دو) هرگاه $h : A \to C$ ریختی با خاصیت $fh = gh$ باشد، آنگاه یک ریخت منحصر به فرد مانند $\bar{h} : A \to B$ وجود دارد به‌طوری که $i\bar{h} = h$.

یک *هم‌هستهٔ تفاضلی* (یا *هم‌مساوی‌ساز*) برای جفت (f,g) ریختی است مانند $j : D \to E$ به‌طوری که

(سه) $jf = jg$ ؛

(چهار) هرگاه $k : D \to F$ ریختی با خاصیت $kf = kg$ باشد، آنگاه یک ریخت منحصر به فرد مانند $\bar{k} : E \to F$ وجود دارد به‌طوری که $\bar{k}j = k$.

چند مثال. در رستهٔ $\mathcal{S}$ مجموعه‌ها، هستهٔ تفاضلی $f : C \to D$ و $g : C \to D$ نگاشت شمول $B \to C$ است، که در آن $B = \{c \in C \mid f(c) = g(c)\}$. همین‌ساختن‌نشان می‌دهد که هر جفت ریخت در رسته‌های گروهها، حلقه‌ها، و مدولها دارای هستهٔ تفاضلی است.

مثال. فرض کنیم $f: G \to H$ و $g: G \to H$ همریختیهای گروهها باشند. همچنین، N کوچکترین زیرگروه نرمال H باشد که شامل $\{f(a)g(a)^{-1} \mid a \in G\}$ است. بنابر قضیهٔ I ۶۰۵۰، بروریختی کانونی $H \to H/N$ یک هم‌هستهٔ تفاضلی است.

حکم ۶۰۳. *فرض کنیم* $f: C \to D$ و $g: C \to D$ *ریختهایی از رستهٔ* $\mathcal{C}$ *باشند.*
(یک) *هرگاه* $i: B \to C$ *یک هستهٔ تفاضلی* (f,g) *باشد، آنگاه* i *یک تکریختی است.*
(دو) *هرگاه* $i: B \to C$ و $j: A \to C$ *هسته‌های تفاضلی* (f,g) *باشند، آنگاه یک تعادل منحصر به فرد مانند* $h: A \to B$ *وجود دارد به‌طوری که* $ih = j$.

برهان. (یک) فرض کنیم $h, k: F \to B$ ریختهایی باشد به‌طوری که $ih = ik$. در این صورت، $f(ih) = (fi)h = (gi)h = g(ih)$. چون i یک هستهٔ تفاضلی (f,g) است، ریخت منحصر به فردی مانند $t: F \to B$ وجود دارد به‌طوری که $it = ih$. اما هر دوی $t = h$ و $t = k$ در این شرط صدق می‌کنند؛ درنتیجه، بنابر یکتایی، $h = k$. بنابراین، i تکین می‌باشد.
(دو) طبق فرض، ریختهای منحصر به فردی چون $h: A \to B$ و $k: B \to A$ وجود دارند به‌طوری‌که $ih = j$ و $jk = i$. درنتیجه، $ihk = jk = i = i \circ 1_B$ و $jkh = ih = j = j \circ 1_A$. چون i و j طبق (یک) تکریختی‌اند، $hk = 1_B$ و $kh = 1_A$. بنابراین، h یک تعادل می‌باشد.

تبصره. هم‌هسته‌های تفاضلی بروریختی بوده و دوگان حکم ۶۰۳ (دو) برای هم‌هسته‌های تفاضلی برقرار است.

فرض کنیم $\mathcal{C}$ رسته‌ای دارای شیٔ صفر 0 و درنتیجه ریختهای صفر باشد (حکم ۴۰۳). هستهٔ ریخت $f: C \to D$ (در صورت وجود) مساوی یک هستهٔ تفاضلی جفت $(f, 0_{C,D})$ تعریف می‌شود؛ این هسته گاهی با $\operatorname{Ker} f$ نموده می‌شود. تعریف ۵۰۳ و احکام ۴۰۳ و ۶۰۳ نشان می‌دهند که $k: K \to C$ یک هستهٔ $f: C \to D$ است اگر و فقط اگر
(یک) k *تکریختی* با خاصیت $fk = 0_{K,D}$ باشد؛ و
(دو) هرگاه $h: B \to C$ یک ریخت باشد به‌طوری که $fh = 0_{B,D}$، آنگاه یک ریخت منحصر

به فرد مانند $\bar{h}: B \to K$ وجود داشته باشد که $k\bar{h} = h$.
بنابر حکم ۶.۳ ، K با تقریب تعادل منحصر به فرد است .

هم‌هستهٔ $t: D \to E$ از یک ریخت $f: C \to D$ به‌طوردوگان‌مساوی‌هم‌هستهٔ تفاضلی جفت $(f, 0_{C,D})$ تعریف می‌شود؛ و گاهی با Coker f نموده خواهد شد . مثل فوق ، t با شرایط‌زیر مشخص خواهد شد :
(سه) t بروریختی با خاصیت $tf = 0_{C,E}$ است؛ و
(چهار) هرگاه $g: D \to F$ یک‌ریخت باشد به‌طوری که $gf = 0_{C,F}$ ، آنگاه ریخت منحصر به فردی مانند $\bar{g}: E \to F$ وجود دارد به‌طوری که $\bar{g}t = g$.

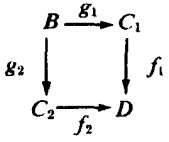
چند مثال . در رسته‌های گروهها ، حلقه‌ها ، و مدولها ، هستهٔ ریخت $f: C \to D$ عبارت است‌ازنگاشت‌شمول $K \to C$ ، که در آن K هستهٔ معمولی‌است و $K = \{c \in C \mid f(c) = 0\}$.
در رستهٔ مدولها ، بروریختی کانونی $D \to D/\mathrm{Im}\, f$ یک هم‌هستهٔ f خواهد بود .

تمرینات

۱ . یک ریخت‌دررستهٔ مجموعه‌ها تکین [بروبی] است‌اگرو فقط‌اگر انژکتیو [سورژکتیو] باشد .

۲ . ریخت $f: G \to H$ در رستهٔ گروهها بروبی است اگر و فقط‌اگر f یک همریختی سورژکتیو (یعنی ، بروریختی‌به‌معنی‌عادی) باشد . [**راهنمایی .** هرگاه f بروبی بوده ، $K = \mathrm{Im}\, f$ ، و $j: K \to H$ نگاشت شمول باشد ، آنگاه ، بنابر حکم ۲.۳ ، j بروبی‌است . به‌طریق زیر نشان دهید که f سورژکتیو است (یعنی ، $K = H$) .
فرض کنید S مجموعهٔ‌هم مجموعه‌های‌چپ K در H باشد؛ همچنین ، $T = S \cup \{u\}$ که در آن $u \notin S$. و نیز A گروه تمام جایگشتهای T باشد . $t: H \to A$ با $t(h)(h'K) = hh'K$ و $t(h)(u) = u$ داده شده است . فرض کنید $s: H \to A$ با $\sigma t(h)\sigma$ تعریف‌شده‌باشد ، که در آن $\sigma \in A$ ترانهشی است که u و K را باهم عوض می‌کند .
نشان دهید که s و t همریختیهایی اند که $sj = tj$ ، که از آنجا $s = t$. نشان دهید به‌ازای هر $h \in H$ ، $hK = K$ ؛ بنابراین ، $K = H$.]

۳ . نمودار تعویضپذیر



از ریختهای رستهٔ $\mathcal{C}$ یک **برگشت** برای f_1 و f_2 نام دارد اگر به‌ازای هر جفت ریخت مانند $h_1 : B' \to C_1$، $h_2 : B' \to C_2$ که $f_1h_1 = f_2h_2$، ریخت منحصر به فردی مانند $t : B' \to B$ موجود باشد که $h_1 = g_1t$ و $h_2 = g_2t$.

(آ) هرگاه نمودار برگشت دیگری برای f_1, f_2 موجود باشد که B_1 گوشهٔ چپ بالایی آن است، آنگاه B و B_1 معادل می‌باشند.

(ب) درنمودار برگشت بالا، هرگاه f_2 تکریختی باشد، آنگاه g_1 نیز چنین‌است.

(پ) هر جفت تابع $f_1 : C_1 \to D, f_2 : C_2 \to D$ در رستهٔ مجموعه‌ها دارای برگشت است.

۴. نشان دهید که هر جفت تابع $f, g : C \to D$ در رستهٔ مجموعه‌ها هم‌هستهٔ تفاضلی دارد.

۵. فرض کنید $f, g : C \to D$ ریختهایی در رستهٔ $\mathcal{C}$ باشند. به‌ازای هر X در $\mathcal{C}$، قرار دهید

$$\mathrm{Eq}(X, f, g) = \{h \in \hom(X, C) \mid fh = gh\}.$$

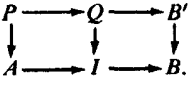
(آ) $\mathrm{Eq}(-, f, g)$ یک تابعگر پادورد از $\mathcal{C}$ به رستهٔ مجموعه‌هاست.

(ب) ریخت $i : K \to C$ یک هستهٔ تفاضلی (f, g) است اگر و فقط اگر $\mathrm{Eq}(-, f, g)$ نمایشپذیر باشی‌نمایندهٔ K باشد (یعنی، یک یکریختی طبیعی مانند

$$\tau : \hom_{\mathcal{C}}(-, K) \to \mathrm{Eq}(-, f, g)$$

وجود داشته باشد). [**راهنمایی.** نشان دهید که به‌ازای $h : X \to K$، $\tau_X(h) = ih$، که در آن $i = \tau_K(1_K)$.]

۶. هرگاه هر مربع نمودار زیر یک برگشت‌بوده و $B \to B'$ یک تکریختی باشد، آنگاه مستطیل خارجی نیز برگشت است. [**راهنمایی.** ر.ک. تمرین ۳.]



۷. در یک رسته دارای شیٔ صفر، هستهٔ هر تکریختی یک ریخت صفر است.

فهرست علایم

علامت	معنی	شمارهٔ صفحه
$\mathbf{Q}$	میدان اعداد گویا	۱
$\mathbf{R}$	میدان اعداد حقیقی	۱
$\mathbf{C}$	میدان اعداد مختلط	۱
$\Rightarrow$	ایجاب می‌کند	۱
$\Leftrightarrow$	اگر و فقط اگر	۱
$\in$	یک عنصر... است	۲
$\notin$	یک عنصر... نیست	۲
$\{x \mid P(x)\}$	ردهٔ تمام xهایی که $P(x)$ راست است	۳
$\subset$	یک زیررده (یازیر مجموعهٔ) ... است	۴
$\varnothing$	مجموعهٔ تهی	۴
$P(A)$ یا 2^A	مجموعهٔ توان A	۴
$\bigcup_{i \in I} A_i$	اجتماع مجموعه‌های A_i	۴
$\bigcap_{i \in I} A_i$	اشتراک مجموعه‌های A_i	۴

$B - A$	متمم نسبی A در B	۴
A'	متمم A	۴
$f: A \to B$	f تابعی از A به B است	۵
$a \mapsto f(a)$	تابع f، a را به $f(a)$ می‌نگارد	۵
$f \mid S$	تحدید تابع f به S	۵
1_A	تابع همانی بر مجموعهٔ A	۵
	نگاشت همانی حلقهٔ A	۱۷۸
gf یا $g \circ f$	تابع مرکب f و g	۵
	ریخت مرکب f و g	۸۱
$\operatorname{Im} f$	نقش تابع f	۴۷،۶
$f^{-1}(T)$	نقش معکوس مجموعهٔ T	۵
$A \times B$	حاصل ضرب دکارتی مجموعه‌های A و B	۱۱
	حاصل ضرب مستقیم گروههای A و B	۴۰
$\sim$	هم ارز است با	۹
	همتوان است با	۲۴
$\bar{a}$	ردهٔ هم ارزی a	۹
$\prod_{i \in I} A_i$	حاصل ضرب خانوادهٔ $\{A_i \mid i \in I\}$ ازاشیاء	۸۳
	حاصل ضرب مستقیم خانوادهٔ $\{A_i \mid i \in I\}$	۲۷۱،۲۰۲،۹۱
	از گروهها (یا حلقه‌ها یا مدولها)	
$\mathbf{Z}$	مجموعهٔ اعداد صحیح	۱۴
$\mathbf{N}$	مجموعهٔ اعداد صحیح نامنفی (اعداد طبیعی)	۱۴
$\mathbf{N}^*$	مجموعهٔ اعداد صحیح مثبت	۱۴
$a \mid b$	a، b را عاد می‌کند	۲۱۱،۱۶
$a \nmid b$	a، b را عاد نمی‌کند	۲۱۱،۱۶
$(a_1, a_2, \ldots, a_n)$	بزرگترین مقسوم علیه مشترک $a_1, \ldots, a_n$	۱۷

$\mathfrak{C}_T$	رستهٔ تشکیل شده از $\mathfrak{C}$ و T	۷۳۸
$0_{C,D}$	ریخت صفر از C به D	۷۵

کتابنامه

تمام کتابها و مقالاتی که در متن به آنها ارجاع شده است ذیلاً لیست شده‌اند. این لیست حاوی کتب دیگری که ممکن است مراجع سودمندی باشند نیز هست. این لیست بهیچوجه کامل نیست و فقط انتخاب مناسبی از کتب انگلیسی در جبر و مباحث مربوط به آن می‌باشد. تقریباً تمام این کتب برای هر کس که بتواند این کتاب را بخواند قابل درک بوده و فقط در بعضی از آنها بخشهایی از این متن پیشنیاز خواهد بود.

برای راحتی خواننده، کتابها بر حسب عنوان رده‌بندی شده‌اند. ولی این رده‌بندی غیرقابل انعطاف نیست. مثلاً، در چند کتاب با عنوان "عمومی"، نظریهٔ گروهها و همچنین نظریهٔ میدانها و نظریهٔ گالوا به طور کامل مطرح شده است. کتب دیگر نظیر [۲۶] و [۳۹] را می‌توان در بیش از یک عنوان جاداد.

کتابها

عمومی

1. Chevalley, C., *Fundamental Concepts of Algebra*. NewYork: Academic Press, Inc., 1956.
2. Faith, C., *Algebra: Rings, Modules and Categories I*. Berlin: Springer-Verlag, 1973.
3. Goldhaber, J. and G. Ehrlich, *Algebra*. New York: The Macmillan Company, 1970.
4. Herstein, I., *Topics in Algebra*. Waltham, Mass.: Blaisdell Publishing Company, 1964.

5. Lang, S., *Algebra*. Reading, Mass.: Addison-Wesley, Publishing Company, Inc., 1965.
6. MacLane, S. and G. Birkhoff, *Algebra*. New York: The Macmillan Company, 1967.
7. Van der Waerden, B. L., *Algebra*. (7th ed., 2 vols.), New York: Frederick Ungar Publishing Co., 1970.

نظریهٔ مجموعه‌ها

8. Eisenberg, M., *Axiomatic Theory of Sets and Classes*. New York: Holt, Rinehart and Winston, Inc., 1971.
9. Halmos, P., *Naive Set Theory*, Princeton, N. J.: D. Van Nostrand Company Inc., 1960.
10. Suppes, P., *Axiomatic Set Theory*. Princeton, N. J.: D. Van Nostrand Company, Inc., 1960.

گروهها

11. Curtis, C. W. and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*. New York: Interscience Publishers, 1962.
12. Dixon, J., *Problems in Group Theory*. Waltham, Mass.: Blaisdell Publishing Company, 1967.
13. Fuchs, L., *Infinite Abelian Groups*. New York: Academic Press, Inc., 1970.
14. Gorenstein, D., *Finite Groups*. New York: Harper and Row, Publishers, 1968.
15. Hall, M., *The Theory of Groups*. New York: The Macmillan Company, 1959.
16. Hall, M. and J. K. Senior, *The Groups of Order* $2^n (n \leq 6)$. New York: The Macmillan Company, 1964.
17. Kaplansky, I., *Infinite Abelian Groups* (2d ed.), Ann Arbor, Mich.: University of Michigan Press, 1969.
18. Kurosh, A. G., *The Theory of Groups* (2 vols.), New York: Chelsea Publishing Company, 1960.
19. Rotman, J., *The Theory of Groups* (2d ed.). Boston: Allyn and Bacon, Inc., 1973.
20. Scott, W. R., *Group Theory*. Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1964.
21. Zassenhaus, H., *The Theory of Groups*. New York: Chelsea Publishing Company, 1958.

حلقه‌ها و مدولها

22. Divinsky, N. J., *Rings and Radicals*. Toronto: University of Toronto Press, 1965.
23. Gray, M., *A Radical Approach to Algebra*. Reading, Mass.: Addison-Wesley Publishing Company, Inc., 1970.

24. Herstein, I. N., *Noncommutative Rings*. Math. Assoc. of America, distributed by J. Wiley, 1968.
25. Jacobson N., *Structure of Rings*. Amer. Math. Soc. Colloq. Publ., vol. 37, 1964.
26. Jans, J., *Rings and Homology*. New York: Holt, Rinehart and Winston, Inc., 1964.
27. Lambek, J., *Lectures on Rings and Modules*. Waltham, Mass.: Blaisdell Publishing Company, 1966.
28. McCoy, N., *Theory of Rings*. New York: The Macmillan Company, 1964.
29. Northcott, D. G., *Lessons on Rings, Modules and Multiplicity*. New York: Cambridge University Press, 1968.

جبر تعویضپذیر

30. Atiyah, M. F. and I. G. MacDonald, *Introduction to Commutative Algebra*. Reading, Mass.: Addison-Wesley Publishing Company, Inc., 1969.
31. Kaplansky, I., *Commutative Rings*. Boston: Allyn and Bacon, Inc., 1970.
32. Larsen, M. and P. J. McCarthy, *Multiplicative Theory of Ideals*. New York: Academic Press, Inc., 1971.
33. Zariski, O. and P. Samuel, *Commutative Algebra* (vols. I and II). Princeton N. J., D. Van Nostrand Company, Inc., 1958. 1960.

جبر همولوژیک

34. Hilton, P. J. and U. Stammbach, *A Course in Homological Algebra*. Berlin: Springer-Verlag, 1971.
35. S. MacLane, *Homology*. Berlin: Springer-Verlag, 1963.

میدانها

36. Artin, E., *Galois Theory*. Notre Dame, Ind.: Notre Dame Mathematical Lectures No. 2 (2d ed.), 1944.
37. Gaal, L., *Classical Galois Theory with Examples*. Chicago: Markham, 1971.
38. Jacobson, N., *Lectures in Abstract Algebra* (vol. III). Princeton, N. J.: D. Van Nostrand Company, Inc., 1964.
39. Kaplansky, I., *Fields and Rings* (2d ed.). Chicago: University of Chicago Press, 1972.
40. McCarthy, P. J., *Algebraic Extensions of Fields*. Waltham, Mass.: Blaisdell Publishing Company, 1966.

جبر خطی و چند خطی

41. Greub, W., *Linear Algebra* (3rd ed.). Berlin: Springer-Verlag, 1967.

42. Greub, W., *Multilinear Algebra*. Berlin: Springer-Verlag, 1967.
43. Halmos, P. R., *Finite Dimensional Vector Spaces* (2d ed.). Princeton, N. J.: D. Van Nostrand Company, Inc., 1958.
44. Jacobson, N., *Lectures in Abstract Algebra* (vol. II). Princeton, N. J.: D. Van Nostrand Company, Inc., 1953.

رسته‌ها

45. MacLane, S., *Categories for the Working Mathematician*. Berlin: Springer-Verlag, 1972.
46. Mitchell, B., *Theory of Categories*. New York: Academic Press, Inc., 1965.
47. Pareigis, B., *Categories and Functors*. New York: Academic Press, Inc., 1970.

نظریهٔ اعداد

48. Artin E., *Algebraic Numbers and Algebraic Functions*. New York: Gordon and Breach, 1967.
49. Lang, S., *Algebraic Number Theory*. Reading Mass.: Addison-Wesley Publishing Company, Inc., 1970.
50. O'Meara, O. T., *Introduction to Quadratic Forms*. Berlin: Springer-Verlag, 1963.
51. Shockley, J. E., *Introduction to Number Theory*. New York: Holt, Rinehart and Winston, Inc., 1967.
52. Weiss E., *Algebraic Number Theory*. New York: McGraw-Hill Inc., 1963.

هندسهٔ جبری

53. Fulton, W., *An Introduction to Algebraic Geometry*. New York: W. A. Benjamin Inc., 1969.
54. Lang, S., *Introduction to Algebraic Geometry*. New York: Interscience Publishers, 1959.
55. MacDonald, I. G., *Algebraic Geometry: Introduction to Schemes*. New York: W. A. Benjamin Inc., 1968.

آنالیز

56. Burrill, C. W., *Foundations of Real Numbers*. New York: McGraw-Hill, Inc., 1967.

57. Hewitt, E. and K. Stromberg, *Real and Abstract Analysis*. Berlin: Springer-Verlag, 1969.

مقالات و یادداشتها

58. Bergman, G., "A Ring Primitive on the Right but Not on the Left," *Proc. Amer. Math. Soc.*, 15 (1964), pp. 473–475; correction, pg. 1000.
59. Cohen, P. J., *Set Theory and the Continuum Hypothesis*, New York: W. A. Benjamin Inc., 1966.
60. Corner, A. L. S., "On a Conjecture of Pierce Concerning Direct Decomposition of Abelian Groups," *Proc. Colloq. on Abelian Groups*, Budapest, 1964, pp. 43–48.
61. Feit, W. and J. Thompson, "Solvability of Groups of Odd Order," *Pac. Jour. Math.*, 13 (1963), pp. 775–1029.
62. Goldie, A. W., "Semiprime rings with maximum condition," *Proc. Lond. Math. Soc.*, 10 (1960), pp. 201–220.
63. Kaplansky, I., "Projective Modules," *Math. Ann.*, 68 (1958), pp. 372–377.
64. Krull, W., "Galoissche Theorie der unendlichen algebraischen Erweiterungen," *Math. Ann.*, 100 (1928), pp. 687–698.
65. Procesi, C. and L. Small, "On a theorem of Goldie," *Jour. of Algebra*, 2 (1965), pp. 80–84.
66. Sasiada, E. and P. M. Cohn, "An Example of a Simple Radical Ring," *Jour. of Algebra*, 5 (1967), pp. 373–377.

واژه‌نامه

فارسی به انگلیسی

آر	R
دور	cycle
مدول	module
آرتینی	artinian
حلقهٔ	ring
مدول	module
آزاد	free
تابعگر	functor
شئ	object
شئ	object
ضرب	product
گروه	group
آبلی	abelian
مدول	module
اثر	trace
اجتماع	union

disjoint	ازهم جدا
valuation	ارزیابی
ring	حلقهٔ
discrete	گسسته
domain	دامنهٔ
induction	استقرا
transfinite	ترانسفینی
mathematical	ریاضی
independence	استقلال
algebraic	جبری
linear	خطی
intersection	اشتراک
principle	اصل
induction	استقرا
transfinite	ترانسفینی
mathematical	ریاضی
of well ordering	خوش ترتیبی
axiom	اصل موضوع (اصل)
of choice	انتخاب
of pair formation	تشکیل جفت
of class formation	تشکیل رده
power	توان
of extensionality	گسترش
principal	اصلی
ideal	ایده‌آل

ring	حلقهٔ
domain	دامنهٔ
cardinality	اصلیت
partition	افراز
ascending	افزایشی
central series	سری مرکزی
chain condition	شرط زنجیر
euclidean	اقلیدسی
algorithm	الگوریتم
ring	حلقهٔ
adjoint	الحاق (ی)
associativity	شرکتپذیری
classical	کلاسیک
adjoining	الحاق
a root	یک ریشه
join	الحاق
of groups	گروهها
algorithm	الگوریتم
euclidean	اقلیدسی
division	بخشی
m-system	m- دستگاه
choice	انتخاب
axiom of	اصل
function	تابع
translation	انتقال

end	انتها
index	اندیس
relative	نسبی
of a subgroup	یک زیر گروه
injective	انژکتیو
function	تابع
module	مدول
injection	انژکسیون
canonical	کانونی
primary	اول
ideal	ایده‌آل
decomposition	تجزیهٔ
submodule	زیرمدول
prime	اول
ideal	ایده‌آل
ring	حلقهٔ
radical	رادیکال
subfield	زیرمیدان
integer	عدد صحیح
element	عنصر
primitive	اولیه
ideal	ایده‌آل
polynomial	چند جمله‌ای
ring	حلقهٔ
root	ریشهٔ

ideal	ایده‌آل
principal	اصلی
prime	اول
isolated	تنها
associated	مربوطه
primitive	اولیه
finitely generated	باتولید متناهی
trivial	بدیهی
nil	پوچ
nilpotent	پوچ توان
left	چپ
modular	مدولی
regular	منتظم
proper	حقیقی
fractional	کسری
maximal	ماکزیمال
range	برد
of a function	یک تابع
vector	بردار
column	ستونی
row	سطری
pullback	برگشت
epimorphism	برووریختی
canonical	کانونی

g.l.b	بزرگترین کران پایینی
multiplicaity	بستایی
of a root	یک ریشه
closed	بسته
subgroup	زیر گروه
object	شیء
operation	عمل
algebraically	به طور جبری
closed	بسته
independent	مستقل
dependent	وابسته
anti-isomorphism	پادیکریختی
p-primary	p-اولیه
invariant	پایا
dimension property	خاصیت بعد
subspace	زیرفضای
factors	عاملهای
stabilizer	پایدارساز
basis	پایه
transcendence	تعالی
separating	جداگر
dual	دوگان
standard	متعارف
p-radical	p-رادیکال

p-گروه	p-group
پوچ (هیچ)	nil
ایده‌آل	ideal
رادیکال	radical
پوچ توان	nilpotent
ایده‌آل	ideal
درونریختی	endomorphism
عنصر	elemnt
گروه	group
پوچی	nullity
پیما	span
تاب	torsion
زیرگروه	subgroup
زیر مدول	submodule
گروه	group
مدول	module
تابع	function
انتخاب	choice
انژکتیو	injective
اویلر	Euler
برو	onto
بیژکتیو	bijective
چند خطی	multilinear
دوخطی	bilinear

surjective	سورژکتیو
rational	گویا
Moebius	موبیوس
functor	تابعگر
representable	قابل نمایش
successor	تالی
immediate	بلافصل
transformation	تبدیل
linear	خطی
natural	طبیعی
decomposition	تجزیه
primary	اولیهٔ
irredundant	غیرزاید
restriction	تحدید
irreducible	تحویل‌ناپذیر
polynomial	چند جمله‌ای
element	عنصر
module	مدول
variety	واریتهٔ
reduced	تحویل یافته
primary decomposition	تجزیهٔ اولیهٔ
row echelon form	شکل سطری پلکانی
word	کلمهٔ
abelian group	گروه آبلی
transpose	ترانهاده

of a matrix	یک ماتریس
transposition	ترانهش
order	ترتیب (مرتبه)
ideal	ایده‌آل
partial	جزئی
left	چپ
ordering	ترتیب
partial	جزئی
linear	خطی
simple	ساده
total	کل
equality	تساوی
equalizer	تساوی ساز
projection	تصویر
canonical	کانونی
refinement	تظریف
of a series	یک سری
equivalence	تعادل
relation	رابطهٔ
class	ردهٔ
natural	طبیعی
transcendence	تعالی
base	پایهٔ
separating	جداگر
degree	درجهٔ

transitive	تعدی (متعدی)
n-fold	nگونا
relation	رابطهٔ
subring	زیر حلقهٔ
subgroup	زیرگروه
monomial	تکجمله‌ای
monomorphism	تکریختی
monoid	تکگون
monic	تکین
polynomial	چند جمله‌ای
morphism	ریخت
paradox	تناقض
power	توان (ی)
axiom	اصل موضوع
series	سری
set	مجموعهٔ
extension	توسیع
separably generated	به طورجدایی‌پذیر تولید شده
abelian field	میدان آبلی
empty	تهی
world	کلمهٔ
set	مجموعهٔ
permutation (s)	جایگشت (ها)
disjoint	از هم جدا

even	زوج
odd	فرد
algebra	جبر(ی)
artinian	آرتینی
ideal	ایده‌آل
division	بخشی
fundamental theorem of	قضیهٔ اساسی
group	گروه
algebraic	جبری
closure	بست
field extension	توسیع میدان
algebra	جبر
number	عدد
element	عنصر
set	مجموعهٔ
separable	جدایی‌پذیر
extension	توسیع
polynomial	چند جمله‌ای
degree	درجهٔ
element	عنصر
inseparable	جدایی ناپذیر
degree	درجهٔ
purely-extension	توسیع صرفاً
pair	جفت
formation	تشکیل

ordered	مرتب
summand	جمعوند
direct	مستقیم
left	چپ
adjoint	الحاق
ideal	ایده‌آل
quotient ring	حلقهٔ خارج قسمتی
annihilator	صفرساز
invertible element	عنصر معکوسپذیر
exact	کامل
order	مرتبهٔ
quasi-regular	منتظم نما
coset	هم مجموعهٔ
polynomial	چند جمله‌ای
primitive	اولیه
irreducible	تحویل ناپذیر
monic	تکین
separable	جدایی پذیر
cyclotomic	دایره بر
degree of	درجهٔ
characteristic	مشخص
minimal	مینیمال
minimum	مینیمم
multilinear	چند خطی

function	تابع
form	فرم
quaternion	چهارتا
product	حاصل ضرب
meaningful	بامعنی
tensor	تانسوری
cartesian	دکارتی
category	رسته‌ای
subdirect	زیر مستقیم
direct	مستقیم
weak	ضعیف
map	نگاشت
semidirect	نیمه مستقیم
cancellation	حذف
proper	حقیقی
ideal	ایده‌آل
vector	بردار
refinement	تظریف
class	ردهٔ
subgroup	زیرگروه
value	مقدار
solvable	حلپذیر
by radicals	به وسیلهٔ رادیکالها
series	سری

group	گروه
ring	حلقهٔ
artinian	آرتینی
euclidean	اقلیدسی
prime	اول
primitive	اولیه
division	بخشی
boolean	بولی
subdirectly irreducible	به طور زیر مستقیم تحویل ناپذیر
integrally closed	به طور صحیح بسته
commutative	تعویضپذیر
of polynomials	چند جمله‌ایها
quotient	خارج قسمتی
left	چپ
endomorphism	درونریختی
radical	رادیکال
simple	ساده
group	گروهی
opposite	متقابل
regular	منتظم
local	موضعی
semisimple	نیمه ساده

quotient	خارج قسمتی
ring	حلقهٔ

class	ردهٔ
group	گروه
field	میدان
linear	خطی
independence	استقلال
functional	تابعی
ordering	ترتیب
combination	ترکیب
algebra	جبر
equation	معادلهٔ
dependence	وابستگی
idempotent (s)	خودتوان (ها)
element	عنصر
orthogonal	متعامد
automorphism	خودریختی
extendible	توسیع پذیر
inner	داخلی
well ordering	خوش ترتیبی
principle	اصل
law of	قانون
domain	دامنه
principal ideal	ایده‌آل اصلی
unique factorization	یکتایی تجزیه
endomorphism (s)	درونریختی (ها)
nilpotent	پوچ توان

ring	حلقهٔ
normal	نرمال
internal	داخلی
product	حاصل ضرب
direct	مستقیم
sum	مجموع
direct	مستقیم
interpolation	درونیابی
sequence	دنباله
excat	کامل
split	تجزیه
short	کوتاه
binomial	دوجمله‌ای
coefficient	ضریب
theorem	قضیهٔ
bimodule	دو مدول
relation	رابطه
antisymmetric	پاد متقارن
transitive	متعدی
symmetric	متقارن
reflexive	منعکس
equivalence	هم ارزی
congruence	همنهشتی
radical	رادیکال

prime	اول
p-	-p
nil	هیچ
right	راست
adjoing	الحاق
ideal	ایده‌آل
quotient ring	حلقهٔ خارج قسمتی
annihilator	صفرساز
invertible element	عنصر معکوسپذیر
quasi-regular	منتظم‌نما
coset	هم مجموعه
rank	رتبه
column	ستونی
class	رده (ای)
axiom of... formation	اصل تشکیل
proper	حقیقی
quoteint	خارج قسمتی
equation	معادلهٔ
equivalence	هم ارزی
classification	رده‌بندی
of finite groups	گروههای متناهی
category	رسته
product	حاصل ضربی
dual	دوگان
opposite	متقابل

concrete	ملموس
morphism	ریخت
monic	تکین
zero	صفر
root	ریشه
multiple	چندگانه
simple	ساده
of unity	واحد
chain	زنجیر
subalgebra	زیر جبر
subring	زیر حلقه
subclass	زیر رده
subspace	زیر فضا
subgroup	زیرگروه
trivial	بدیهی
closed	بسته
fully invariant	به طور کامل پایا
commutator	تعویضگر
proper	حقیقی
cyclic	دوری
transitive	متعدی
derived	مشتق
characteristic	مشخص
normal	نرمال

maximal	ماکزیمال
minimal	مینیمال
subset	زیر مجموعه
submodule	زیر مدول
primary	اولیه
finitely generated	باتولید متناهی
torsion	تابی
cyclic	دوری
subfield	زیرمیدان
prime	اول
linearly disjoint	به طور خطی از هم جدا
maximal	ماکزیمال
composite	مرکب
predecessor	سابق
immediate	بلافصل
simple	ساده
ordering	ترتیب
ring	حلقهٔ
root	ریشهٔ
group	گروه
module	مدول
series	سری (ها)
composition	ترکیب
power	توانی

formal	صوری
solvable	حلپذیر
subnormal	زیرنرمال
central	مرکزی
ascending	افزایشی
equivalent	معادل
normal	نرمال
row	سطر (ی)
vector	بردار
rank	رتبهٔ
form	شکل
echelon	پلکانی
operation	عمل
elementary	مقدماتی
space	فضای
lattice	شبکه
complete	تام
condition	شرط
chain	زنجیر
ascending	افزایشی
maximum	ماکزیمم
associative	شرکتپذیر (ی)
binary operation	عملی دوتایی
law	قانون

associate	شریک
object	شیء
initial	اولیه
terminal	نهایی
integral	صحیح
closure	بست
ring extension	توسیع حلقهٔ
domain	دامنهٔ
element	عنصر
purely	صرفاً
inseparable	جدایی ناپذیر
extension	بسط
element	عنصر
transcendental	متعالی
extension	بسط
zero	صفر
element	عنصر
matrix	ماتریس
divisor	مقسوم علیه
annihilator	صفرساز
formal	صوری
power series	سری توانی
derivative	مشتق

coefficient	ضریب
leading	پیشرو
natural	طبیعی
transformation	تبدیل
number	عدد
homomorphism	همریختی
isomorphism	یکریختی
length	طول
of a series	یک سری
spectrum	طیف
number	عدد
cardinal	اصلی
natural	طبیعی
integer	عدد صحیح
modulo m	به پیمانهٔ m
gaussian	گاوسی
memership	عضویت
sign	علامت
of a permutation	یک جایگشت
operation	عمل
binary	دوتایی
column	ستونی
row	سطری

elementary	مقدماتی
group	گروه
university	عمومی
mapping property	خاصیت نگاشت
object	شیء
element	عنصر
torsion-free	فارغ از تاب
group	گروه
module	مدول
law	قانون
trichotomy	تثلیث
of well ordering	خوش ترتیبی
theorem	قضیه
fundamental	اساسی
of algebra	جبر
of arithmetic	حساب
recursion	بازگشتی
remainder	باقیمانده
chinese	چینی
lying-over	روقرار دادن
intermediate value	مقدار میانی
isomorphism	یکریختی
second	دوم

third	سوم
diagonal	قطر
main	اصلی
K-algebra	K- جبر
canonical	کانونی
injection	انژکسیون
epimorphism	برو ریختی
projection	تصویر
form	شکل
rational	گویای
map	نگاشت
linear	خطی
bilinear	دو خطی
K-homomorphism	K-همریختی
bound	کران
upper	بالایی
least	کوچکترین
lower	پایینی
greatest	بزرگترین
least	کوچکترین
element	عنصر
bound	کران
upper	بالایی
total	کل

ترتیب	ordering
درجهٔ	degree
کلمه	word
تحویل یافته	reduced
تهی	empty
کوتاه	short
دنباله	sequence
کامل	exact
لم پنج	five lemma
گروه	group
آبلی	abelian
آزاد	free
باتولید متناهی	finitely generated
بخشپذیر	divisible
تجزیه ناپذیر	indecomposable
چهارگان	four
ماوراءدوری	metacyclic
یکسویی	isotropy
گویا (ها)	rational (s)
به پیمانهٔ یک	modulo one
تابع	function
متقارن	symmetric
شکل	form
کانونی	canonical

lemma	لم
normalization	نرمال سازی
matrix (matrices)	ماتریس (ها)
secondary	ثانوی
similar	متشابه
symmetric	متقارن
skew	اریب
triangular	مثلثی
equivalent	معادل
invertible	معکوسپذیر
elementary	مقدماتی
companion	همراه
maximal	ماکزیمال
ideal	ایده‌آل
subgroup	زیرگروه
normal	نرمال
subfield	زیرمیدان
element	عنصر
standard	متعارف
basis	پایهٔ
product	حاصل ضرب
transcendental	متعالی
extension	توسیع
purely	صرفاً

element	عنصر
opposite	متقابل
ring	حلقهٔ
category	رستهٔ
symmetric	متقارن
skew	اریب
form	فرم
matrix	ماتریس
function	تابع
multilinear	چند خطی
group	گروه
matrix	ماتریس
complement	متمم
relative	نسبی
alternating	متناوب
function	تابع
multilinear	چند خطی
group	گروه
sum	مجموع
direct	مستقیم
set (s)	مجموعه (ها)
disjoint	از هم جدا
null	پوچ
power	توان
empty	تهی

well ordered خوش ترتیب
underlying زمینه
denumerable شمارشپذیر
multiplicative ضربی
finite متناهی
ordered مرتب
partially جزئی
linearly خطی
equipollent همتوان
orbit مدار
of a permutation یک جایگشت
module مدول
artinian آرتینی
free آزاد
injective انژکتیو
trivial بدیهی
torsion تابی
reducible تحویلپذیر
completely کاملاً
projective تصویری
algebra جبری
dual دوگان
rank of رتبهٔ
simple ساده
torsion-free فارغ از تاب

reflexive	منعکس
noetherian	نوتری
semisimple	نیمه ساده
faithful	وفادار
unitary	یکه‌ای
center	مرکز
of a ring	یک حلقه
of a group	یک گروه
centralizer	مرکزساز
central	مرکزی
division	بخش
simple	سادهٔ
algebra	جبر
independent	مستقل
linearly	خطی
characteristic	مشخص
vector	بردار
subgroup	زیرگروه
space	فضای
value	مقدار
equivalent	معادل
series	سریهای
matrices	ماتریسهای
equation	معادله
linear	خطی

general	کلی
inverse	معکوس
two sided	دوطرفه
image	نقش
invertible	معکوسپذیر
element	عنصر
matrix	ماتریس
cubic	مکعبی
resolvant	حلال
regular	منتظم
ideal	ایده‌آل
left	چپ
function	تابع
ring	حلقهٔ
element	عنصر
quasi	نما
logic	منطق
reflexive	منعکس
relation	رابطهٔ
module	مدول
singleton	منفرد
localization	موضعی سازی
indeterminate	میانی
field	میدان
splitting	تجزیه گر

توسیع	extension
آبلی	abelian
به طور جدایی پذیر تولید شده	separably generated
جبری	algebraic
جدایی پذیر	separable
دایره بر	cyclotomic
دوری	cyclic
رادیکال	radical
ساده	simple
صرفاً جدایی ناپذیر	separably generated
صرفاً متعالی	purely transcendental
متعالی	transcendental
نرمال	normal
کامل	perfect
میانی	intermediate
بسته	closed
پایدار	stable
مینور	minor
یک ماتریس	of a matrix
مینیمال	minimal
ایده‌آل	ideal
اول	prime
چپ	left
چند جمله‌ای	polynomial
زیر گروه	subgroup

normal	نرمال
annihilator	صفرساز
element	عنصر
minimum	مینیمم
polynomial	چند جمله‌ای
condition	شرط
element	عنصر
norm	نرم
normal	نرمال
closure	بست
endomorphism	درونریختی
subgroup	زیرگروه
series	سری
extension	میدان توسیع
normalizer	نرمال ساز
relatively prime	نسبت به هم اول
integers	اعداد صحیح
ring elements	عنصرهای حلقه
relative	نسبی
index	اندیس
dimension	بعد
embedding	نشاننده
image	نقش
inverse	معکوس

map	نگاشت
linear	خطی
middle	میانی
bilinear	دوخطی
canonical	کانونی
inclusion	شمول
quasi	نما
inverse	معکوس
regular	منتظم
notation	نماد
additive	جمعی
presentation	نمایش
of a group	یک گروه
exponentiation	نماگیری
noetherian	نوتری
ring	حلقهٔ
module	مدول
semigroup	نیمگروه
semisimple	نیمه ساده
ring	حلقهٔ
module	مدول
unity	واحد
root of	ریشهٔ
primitive	اولیهٔ

variety	واریته
affine	مستوی
kernel	هسته
difference	تفاضلی
of a morphism	یک ریخت
identity	همانی
function	تابع
functor	تابعگر
matrix	ماتریس
homomorphism	همریختی
induced	القایی
substitution	جانشانی
natural	طبیعی
homogeneous	همگن
of degree k	از درجهٔ k
one-to-one	یک به یک
function	تابع
correspondence	تناظر
isomorphism	یکریختی
natural	طبیعی
unit	یکه
map	نگاشت

واژه‌نامه

انگلیسی به فارسی

abelian	آبلی
field extension	توسیع میدان
group	گروه
divisible	بخشپذیر
finitely generated	باتولید متناهی
free	آزاد
action	عمل
of group on set	گروه برمجموعه
additive	جمعی
notation for groups	نماد برای گروههای
adjoining	الحاق
a root	یک ریشه
adjoint	الحاقی
associativity	شرکتپذیری
pair of functors	جفت . . . از عملگرها
affine	مستوی
variety	واریتهٔ

algera	جبر (ی)
division	بخشی
fundamental theorem	قضیهٔ اساسی
group	گروه
ideal	ایده‌آل
left artinian	آرتینی چپ
algebraic	جبری
algebra	جبر
closure	بست
element	عنصر
field extension	توسیع میدان
number	عدد
set	مجموعهٔ
algebraically	به طور جبری
closed field	میدان . . . بسته
(in) dependent	(مستقل) وابسته
algorithm	الگوریتم
division	تقسیم
euclidean	اقلیدسی
alternating	متناوب
group	گروه
multilinear function	تابع چند خطی
annihilator	صفرساز
anti-isomorphism	پادیکریختی
antisymmetric	پادمتقارن

relation	رابطهٔ
artinian	آرتینی
left . . . algebra	جبر . . . چپ
module	مدول
ring	حلقهٔ
ascending	افزایشی
central series	سری مرکزی
chain condition	شرط زنجیر
associate	شریک
associated	مربوطه
prime ideal	ایده‌آل اول
associative	شرکتپذیری (ی)
binary operation	عمل دوتایی
generalized . . . law	قانون . . . تعمیم یافته
automorphism	خودریختی
extendible	توسیع‌پذیر
inner	داخلی
axiom	اصل (موضوع)
of choice	انتخاب
of class formation	تشکیل رده
of extensionality	گسترش
of pair formation	تشکیل جفت
power	توان
base	پایه

trascendence	متعالی
basis	پایه
dual	دوگان
standard	متعارف
trascendence	متعالی
bijective	بیژکتیو
function	تابع
bilinear	دوخطی
map	نگاشت
canonical	کانونی
bimodule	دومدول
binary	دوتایی
operation	عمل
binomial	دوجمله‌ای
coefficient	ضریب
theorem	قضیهٔ
boolean	بولی
ring	حلقهٔ
bound	کران
greatest lower	بزرگترین . . . پایینی
least upper	کوچکترین . . . بالایی
upper	بالایی
cancellation	حذف
canonical	کانونی

bilinear	دوخطی
map	نگاشت
epimorphism	برووریختی
form	شکل
injection	انژکسیون
middle linear	خطی میانی
map	نگاشت
primary rational	گویای اولیه
form	شکل
projection	تصویر
rational	گویا
form	شکل
cardinal	اصلی
number	عدد
cardinality	اصلیت
category	رسته
concrete	واقعی
dual	دوگان
opposite	متقابل
product	حاصل ضربی
center	مرکز
of a group	یک گروه
of a ring	یک حلقه
central	مرکزی
ascending . . . series	سری . . . افزایشی

idempotent	خودتوان
simple division	بخش سادهٔ
algebra	جبر
centralizer	مرکزساز
chain	زنجیر
condition	شرط
characteristic	مشخص
of a ring	یک حلقه
polynomial	چند جمله‌ای
vector	بردار
value	مقدار
space	فضای
subgroup	زیرگروه
choice	انتخاب
axiom of	اصل موضوع
function	تابع
class	رده
axiom of . . . formation	اصل تشکیل
equation	معادلهٔ
equivalence	هم ارزی
proper	حقیقی
quotient	خارج قسمتی
classical	کلاسیک
adjoint	الحاقی
classification	رده‌بندی

of finite groups	گروههای متناهی
closed	بسته
intermediate field	میدان میانی
object	شیء
subgroup	زیرگروه
closure	بست
algebraic	جبری
integral	انتگرالی
normal	نرمال
codomain	هم دامنه
coequalizer	هم مساوی ساز
cofactor	همعامل
coimage	هم نقش
cokernel	هم هسته
column	ستون (ی)
elementary . . . operation	عمل . . . مقدماتی
rank	رتبهٔ
space	فضای
vector	بردار
commutative	تعویضپذیر (ی)
binary operation	عمل دوتایی
diagram	نمودار
generalized . . . law	قانون . . . تعمیم یافته
group	گروه
ring	حلقهٔ

commutator	تعویضگر
subgroup	زیرگروه
companion	همراه
matirx	ماتریس
comparable	قیاسپذیر
elements	عنصرهای
complement	متمم
complete	تام
direct sum	مجموع مستقیم
lattice	شبکهٔ
ring of quotients	حلقهٔ خارج قسمتهای
set of . . . cosets	مجموعهٔ هم مجموعه‌های
representative	نمایندهٔ
completely	به طور تام
reducible	تحویل پذیر
module	مدول
composite	مرکب
function	تابع
functor	تابعگر
morphism	ریخت
subfield	زیرمیدان
concrete	ملموس
category	رستهٔ
congruence	همنهشتی
modulo m	به پیمانهٔ m

modulo a subgroup	به پیمانهٔ یک زیر گروه
relation	رابطهٔ
conjugacy	ازدواج
class	ردهٔ
conjugate	مزدوج
elements	عنصرهای
subgroups	زیرگروههای
conjugation	تزویج
constant	ثابت
polynomial	چند جمله‌ای
term	جملهٔ
constructible	ساختنی
number	عدد
content	احتوا
of a polynomial	یک چند جمله‌ای
continuum	پیوستار
hypothesis	فرض
contraction	انقباض
of an ideal	یک ایده‌آل
contravariant	پادورد
functor	تابعگر
hom	hom
coordinate	مختص (ات)
ring	حلقهٔ
coproduct	هم حاصل ضرب

correspondence	تناظر
Galois	گالوا
coset	هم مجموعه
representative	نمایندهٔ
couniversal	هم عمومی
object	شیء
covariant	هممورد
functor	تابعگر
hom	hom
cubic	مکعبی
resolvant	حلال
cycle	دور
disjoint	از هم جدا
cyclic	دوری
field extension	توسیع میدان
group	گروه
module	مدول
subspace	زیرفضا
cyclotomic	دایره بر
extension	توسیع
polynomial	چند جمله‌ای
degree	درجه
of a field element	یک عنصر میدان
of inseparability	جدایی ناپذیری

of a polynomial	یک چند جمله‌ای
transcendence	تعالی
delta	دلتا
dense	چگال
ring	حلقهٔ
density	چگالی
theorem	قضیهٔ
denumerable	شمارشپذیر
set	مجموعهٔ
dependence	وابستگی
algebraic	جبری
linear	خطی
derivative	مشتق
derived	مشتق
subgroup	زیرگروه
descending	کاهشی
chain	زنجیر
condition	شرط
determinant	دترمینان
of an endomorphism	یک درونریختی
diagonal	قطر (ی)
matrix	ماتریس
diagram	نمودار
commutative	تعویضپذیر
difference	تفاضل (ی)

kernel	هسته
cokernel	هم هستهٔ
dihedral	دووجهی
group	گروه
dimension	بعد
relative	نسبی
invariant . . . property	خاصیت . . . پایا
direct	مستقیم
factor	عامل
product	حاصل ضرب
sum	مجموع
summand	جمعوند
discriminant	مبین
discrete	گسسته
valuation	ارزیابی
disjoint	از هم جدا
linearly . . . subfields	میدانهای به طور خطی
permutations	جایگشتهای
sets	مجموعه‌های
union	اجتماع
divisible	بخشپذیر
group	گروه
division	بخش (ی)
algebra	جبر
algorithm	الگوریتم

ring	حلقهٔ
finite	متناهی
divisor	مقسوم علیه
elementary	مقدماتی
greatest common	بزرگترین . . . مشترک
zero	صفر
domain	دامنه
euclidean	اقلیدسی
integral	صحیح
of a function	یک تابع
principal ideal	ایده‌آل اصلی
valuation	ارزیابی
unique factorization	یکتایی تجزیه
double	مضاعف
dual	دوگان
dual	دوگان
basis	پایهٔ
category	رستهٔ
double	مضاعف
map	نگاشت
module	مدول
statement	حکم
echelon	پلکانی
reduced row . . . form	شکل سطری . . . تحویل یافته

eigenspace	فضای ویژه
eigenvalue	مقدار ویژه
eignvector	بردار ویژه
elementary	مقدماتی
column operation	عمل ستونی
divisor	مقسوم علیه
row operation	عمل سطری
symmetric function	تابع متقارن
transformation matrix	ماتریس تبدیل
embedded	نشانیده
prime	اول
embedding	نشاننده
empty	تهی
set	مجموعهٔ
word	کلمهٔ
endomorphism	درونریختی
nilpotent	پوچ توان
normal	نرمال
ring	حلقهٔ
epic	برویی
morphism	ریخت
epimorphism	برووریختی
canonical	کانونی
equality	تساوی
equalizer	مساوی ساز

equation	معادلهٔ
general	کلی
linear	خطی
equipollent	همتوان
sets	مجموعه‌های
equivalence	هم ارزی
class	ردهٔ
natural	طبیعی
relation	رابطهٔ
equivalent	هم ارز
matrices	ماتریسهای
series	سریهای
euclidean	اقلیدسی
algorithm	الگوریتم
ring	حلقهٔ
evaluation	ارزیابی
homomorphism	هـــــمریختی
even	زوج
permutation	جایگشت
exact	کامل
sequence	دنبالهٔ
short	کوتاه
split	تجزیه
exponentiation	نماگیری
in a group	در یک گروه

of cardinal numbers	اعداد اصلی
extendible	توسیع پذیر
automorphism	خودریختی
extension	توسیع
field	میدان
abelian	آبلی
algebraic	جبری
cyclic	دوری
cyclotomic	دایره بر
finitely generated	باتولید متناهی
normal	نرمال
purely inseparable	صرفاً جدایی‌ناپذیر
purely transcendental	صرفاً متعالی
radical	رادیکال
separable	جدایی پذیر
separably generated	به طور جدایی پذیر تولید شده
simple	ساده
transcendental	متعالی
integral	انتگرالی
of an ideal	یک ایده‌آل
ring	حلقه
extensionality	گسترش
axiom of	اصل
external	خارجی

direct sum	مجموع مستقیم
direct product	حاصل ضرب مستقیم
weak	ضعیف
factor	عامل (ی)
group	گروه
invariant	پایا
factorization	تجزیه
unique	یکتایی
faithful	وفادار
module	مدول
field	میدان
algebrically closed	به طور جبری بسته
extension	توسیع
finite	متناهی
fixed	ثابت
intermediate	میانی
perfect	کامل
splitting	تجزیه گر
finite	متناهی
dimensional	بابعد
algebra	جبر
field extension	توسیع میدان
vector space	فضای برداری
field	میدان

group	گروه
set	مجموعهٔ
finitely	متناهی
generated	باتولید
abelian group	گروه آبلی
extension field	توسیع میدان
group	گروه
ideal	ایده‌آل
module	مدول
five	پنج
lemma	لم
fixed	ثابت
field	میدان
forgetful	فراموشی
functor	تابعگر
form	فرم
multilinear	چند خطی
rational canonical	کانونی گویا
primary	اولیه
formal	صوری
derivative	مشتق
power series	سری توانی
four	چهار (گان)
group	گروه
fractional	کسری

ideal	ایده‌آل
free	آزاد
abelian	آبلی
group	گروه
module	مدول
object functor	تابعگر ... شیء
product	ضرب
fully	کاملاً
invariant	پایا
subgroup	زیرگروه
function	تابع
bijective	بیژکتیو
bilinear	دوخطی
choice	انتخاب
injective	انژکتیو
multilinear	چند خطی
surjective	سورژکتیو
symmetric rational	گویای متقارن
functor	تابعگر
adjoint	الحاقی
composite	مرکب
forgetful	فراموشی
free object	آزاد شیء
representable	نمایشپذیر
fundamental	اساسی (اصلی)

theorem	قضیهٔ
of algebra	جبر
of arithmetic	حساب
gaussian	گاوسی
integer	عدد صحیح
general	کلی
equation	معادلهٔ
of degree n	از درجهٔ n
polynomial	چند جمله‌ای
of degree n	از درجهٔ n
generalized	تعمیم یافته
associative	شرکتپذیری
law	قانون
commutative	تعویضپذیری
law	قانون
multiplicative	ضربی
system	دستگاه
generator	مولد
of a group	یک گروه
of an ideal	یک ایده‌آل
of a module	یک مدول
going-up	بالا رفتن
theorem	قضیهٔ
graph	نمودار

greatest	بزرگترین
common divisor	مقسوم علیه مشترک
lower bound	کران پایینی
group	گروه
abelian	آبلی
algebra	جبر
alternating	متناوب
cyclic	دوری
dihedral	دووجهی
divisible	بخشپذیر
factor	عاملی
finite	متناهی
finitely generated	باتولید متناهی
free	آزاد
abelian	آبلی
indecomposable	تجزیه ناپذیر
isomorphic	یکریخت
isotropy	یکسویی
join of	الحاق
metacyclic	ماوراء دوری
nilpotent	پوچ توان
reduced	تحویل یافته
ring	حلقهٔ
simple	ساده
solvable	حلپذیر

symmetric	متقارن
torsion	تابی
homogeneous	همگن
of degree k	از درجهٔ k
system of equations	دستگاه معادلات
homomorphism	همریختی
induced	القایی
natural	طبیعی
substitution	جانشانی
ideal	ایده‌آل
algebra	جبر
finitely generated	باتولید متناهی
fractional	کسری
invertible	معکوسپذیر
maximal	ماکزیمال
nil	پوچ
nilpotent	پوچ توان
order	مرتب
primary	اولیه
prime	اول
primitive	اولیه
principal	اصلی
ring	حلقهٔ

proper	حقیقی
regular left	چپ منتظم
idempotents (s)	خود توان (ها)
element	عنصر
orthogonal	متعامد
identity	همانی
function	تابع
functor	تابعگر
matrix	ماتریس
image	نقش
inverse	معکوس
inclusion	شمول
map	نگاشت
indecomposable	تجزیه ناپذیر
group	گروه
independence	استقلال
algebraic	جبری
linear	خطی
independent	مستقل
set of ideals	مجموعهٔ ایده‌آلهای
indeterminate	مجهول
index	اندیس
relative	نسبی
induced	القایی
homomorphsim	همریختی

induction	استقرا
mathematical	ریاضی
transfinite	ترانسفینی
infinite	نامتناهی
set	مجموعهٔ
initial	اولیه
object	شیء
injection	انژکسیون
canonical	کانونی
injective	انژکتیو
function	تابع
module	مدول
inner	داخلی
automorphism	خودریختی
inseparable	جدایی ناپذیر (ی)
degree	درجهٔ
purely	صرفاً
extension	توسیع
integer	عدد صحیح
gaussian	گاوسی
modulo m	به پیمانهٔ m
integral	صحیح
closure	بست
domain	دامنهٔ
element	عنصر

ring extension	توسیع حلقهٔ
integrally	به طور صحیح
closed	بسته
ring	حلقهٔ
intermediate	میانی
field	میدان
closed	بسته
stable	پایدار
value	مقدار
theorem	قضیهٔ
internal	داخلی
direct	مستقیم
product	حاصل ضرب
sum	مجموع
interpolation	درونیابی
intersection	اشتراک
invariant	پایا
dimension property	خاصیت بعد
factors	عاملهای
subspace	زیرفضای
inverse	معکوس
image	نقش
two sided	دوطرفه
invertible	معکوسپذیر
element	عنصر

fractional	کسری
ideal	ایده‌آل
matrix	ماتریس
irreducible	تحویل ناپذیر
element	عنصر
module	مدول
polynomial	چند جمله‌ای
variety	واریتهٔ
irredundant	غیر زاید
primary	اولیهٔ
decomposition	تجزیهٔ
isolated	تنها
prime	اول
ideal	ایده‌آل
isomorphism	یکریختی
natural	طبیعی
isotropy	یکسویی
group	گروه
join	الحاق
of groups	گروهها
K-	-K
algebra	جبر
homomorphism	همریختی

kernel	هسته
difference	تفاضلی
lattice	شبکه
complete	تام
law	قانون
of well ordering	خوش ترتیبی
leading	پیشرو
coefficient	ضریب
least	کوچکترین
element	عنصر
upper bound	کران بالایی
left	چپ
adjoint	الحاق
annihilator	صفرساز
coset	هم مجموعه
exact	کامل
ideal	ایده‌آل
inverse	معکوس
invertible	معکوسپذیر
element	عنصر
order	مرتبهٔ
quasi-regular	منتظم نما
quotient ring	حلقهٔ خارج قسمتی
length	طول

of a series	یک سری
linear	خطی
algebra	جبر
combination	ترکیب
dependence	وابستگی
equation	معادلهٔ
functional	کسری
independence	استقلال
ordering	ترتیب
transformation	تبدیل
linearly	به طور خطی
disjoint	از هم جدا
subfields	زیر میدانهای
independent	مستقل
automorphisms	خودریختیهای
elements	عنصرهای
local	موضعی
ring	حلقهٔ
localization	موضعی سازی
logic	منطق
lower	پایینی
bound	کران
lying-over	روقرارداشتن
theorem	قضیهٔ

m-system	m-دستگاه
main	اصلی
diagonal	قطری
map	نگاشت
mathematical	ریاضی
induction	استقرای
matrix (ces)	ماتریس (ها)
companion	همراه
determinant	دترمینان
elementary	مقدماتی
equivalent	معادل
invertible	معکوسپذیر
secondary	ثانوی
similar	متشابه
symmetric	متقارن
skew	اریب
triangular	مثلثی
maximal	ماکزیمال
element	عنصر
ideal	ایده‌آل
normal subgroup	زیرگروه نرمال
subfield	زیر میدان
maximum	ماکزیمم
condition	شرط
meaningful	با معنی

product	حاصل ضرب
membership	عضویت
metacyclic	ماوراء دوری
group	گروه
middle linear	خطی میانی
map	نگاشت
canonical	کانونی
minimal	مینیمال
annihilator	صفرساز
element	عنصر
left ideal	ایده‌آل چپ
normal subgroup	زیرگروه نرمال
polynomial	چند جمله‌ای
prime ideal	ایده‌آل اول
minimum	مینیمم
condition	شرط
element	عنصر
polynomial	چند جمله‌ای
minor	مینور
of a matrix	یک ماتریس
modular	مدولی
left ideal	ایده‌آل چپ
module	مدول
algebra	جبر
artinian	آرتینی

completely reducible	کاملاً تحویلپذیر
dual	دوگان
faithful	وفادار
free	آزاد
injective	انژکتیو
noetherian	نوتری
projective	تصویری
reflexive	منعکس
semisimple	نیمه ساده
simple	ساده
torsion	تابی
free	آزاد
trivial	بدیهی
unitary	یکه‌ای
monic	تکین
morphism	ریخت
polynomial	چند جمله‌ای
monoid	تکگون
monomial	تکجمله‌ای
monomorphism	تکریختی
morphism	ریخت
epic	برویی
monic	تکین
zero	صفر
multilinear	چند خطی

form	فرم
function	تابع
multiple	چندگانه
root	ریشهٔ
multiplicative	ضربی
set	مجموعهٔ
multiplicity	بستایی
of a root	یک ریشه
n-th root	ریشهٔ nم
of unity	واحد
n-fold	nگویا
transitive	متعدی
natural	طبیعی
homomorphism	همریختی
isomorphism	یکریختی
number	عدد
transformation	تبدیل
nil	پوچ (هیچ)
ideal	ایده‌آل
radical	رادیکال
nilpotent	پوچ توان
element	عنصر
endomorphism	درونریختی
group	گروه

ideal	ایده‌آل
noetherian	نوتری
module	مدول
ring	حلقهٔ
nonsingular	نامنفرد
matrix	ماتریس
norm	نرم
normal	نرمال
closure	بست
endomorphism	درونریختی
extension field	میدان توسیع
series	سری
subgroup	زیرگروه
normalization	نرمال سازی
lemma	لم
normalizer	نرمال ساز
null	پوچ
set	مجموعهٔ
nullity	پوچی
number	عدد
cardinal	اصلی
natural	طبیعی
object	شیء
initial	اولیه

terminal	نهایی
odd	فرد
permutation	جایگشت
one-to-one	یک به یک
correspondence	تناظر
function	تابع
onto	برو
function	تابع
operation	عمل
binary	دوتایی
elenentary	مقدماتی
column	ستونی
row	سطری
opposite	متقابل
category	رستهٔ
ring	حلقهٔ
orbit	مدار
of a permutation	یک جایگشت
order	ترتیب (مرتب)
ideal	ایده‌آل
left	چپ
partial	جزئی
ordered	مرتب
pair	جفت
ordering	ترتیب

by extension	به وسیلهٔ توسیع
linear	خطی
partial	جزئی
simple	ساده
total	کل
orthogonal	متعامد
idempotents	خودتوانهای

p-	-p
group	گروه
primary	اولیه
radical	رادیکال
pair	جفت
formation	تشکیل
ordered	مرتب
partial	جزئی
ordering	ترتیب
partition	افراز
perfect	کامل
field	میدان
permutation (s)	جایگشت (ها)
disjoint	ازهم جدا
even	زوج
odd	فرد
polynomial	چند جمله‌ای

characteristic	مشخص
cyclotomic	دایره‌بر
general	کلـی
irreducible	تحویل ناپذیر
minimal	مینیمال
minimum	مینیمم
monic	تکین
primitive	اولیه
separable	جدایی پذیر
power	توان (ی)
axiom	اصل موضوع
series	سری
set	مجموعهٔ
predecessor	سابق
immediate	بلافصل
presentation	نمایش
of a group	یک گروه
primary	اولیه
decomposition	تجزیهٔ
ideal	ایده‌آل
p- . . . ideal	p-ایده‌آل
p- . . . submodule	p- زیر مدول
rational canonical form	شکل کانونی گویا
submodule	زیر مدول
prime	اول

associated . . . ideal ایده‌آل . . . مربوطه
element عنصر
embedded . . . ideal ایده‌آل . . . نشانیده شده
ideal ایده‌آل
integer عدد صحیح
isolated . . . ideal ایده‌آل . . . تنها
minimal . . . ideal ایده‌آل . . . مینیمال
radical رادیکال
relatively . . . integers اعداد صحیح نسبت به هم
relatively . . . elements عنصرهای نسبت به هم
ring حلقهٔ
subfield زیر میدان
primitive اولیه
element عنصر
ideal ایده‌آل
polynomial چندجمله ای
ring حلقهٔ
root ریشهٔ
of unity واحد
principal اصلی
ideal ایده‌آل
ring حلقهٔ
domain دامنهٔ
module مدول
principle اصل

of mathematical induction	استقرای ریاضی
of transfinite induction	استقرای ترانسفینی
of well ordering	خوش ترتیبی
product	حاصل ضرب (ی)
cartesian	دکارتی
category	رستهٔ
direct	مستقیم
map	نگاشت
semidirect	نیمه مستقیم
subdirect	زیر مستقیم
weak direct	مستقیم ضعیف
projection	تصویر
canonical	کانونی
projective	تصویری
module	مدول
proper	حقیقی
class	ردهٔ
ideal	ایده‌آل
refinement	تظریف
subgroup	زیرگروه
value	مقدار
vector	بردار
pullback	برگشت
purely	صرفاً
inseparable	جدایی ناپذیر

element	عنصر
extension	توسیع
transcendental	متعالی
extension	توسیع

quasi	نما
inverse	معکوس
regular	منتظم
quaternion	چهارتا
quotient	خارج قسمت (ی)
class	رده
field	میدان
group	گروه
ring	حلقهٔ

R-	-R
cycle	دور
module	مدول
radical (s)	رادیکال (ها)
extension field	میدان توسیع
nil	هیچ
p-	-p
prime	اول
property	خاصیت
ring	حلقهٔ

solvable by	حلپذیربه وسیلهٔ
range	برد
of a function	یک تابع
rank	رتبه
column	ستونی
row	سطری
rational	گویا
canonical form	شکل کانونی
function	تابع
symmetric	متقارن
modulo one	به پیمانهٔ یک
recursion	بازگشتی
theorem	قضیهٔ
reduced	تحویل یافته
abelian group	گروه آبلی
primary decomposition	تجزیهٔ اولیهٔ
row echelon form	شکل سطری پلکانی
word	کلمهٔ
refinement	تظریف
of a series	یک سری
reflexive	منعکس
module	مدول
relation	رابطهٔ
regular	منتظم
element	عنصر

function	تابع
left	چپ
ideal	ایده‌آل
quasi	نمای
relation	رابطه
antisymmetric	پادمتقارن
congruence	همنهشتی
equivalence	هم ارزی
refelexive	منعکس
symmetric	متقارن
transitive	متعدی
relative	نسبی
complement	متمم
dimension	بعد
index	اندیس
relatively prime	نسبت به هم اول
integers	اعداد صحیح
ring elements	عناصر حلقه
remainder	باقیمانده
theorem	قضیهٔ
chinese	چینی
representable	نمایش پذیر
functor	تابعگر
representation	نمایش
resolvant	حلال

cubic	مکعبی
restriction	تحدید
right	راست
adjoint	الحاقی
annihilator	صفرساز
coset	هم مجموعهٔ
ideal	ایده‌آل
inverse	معکوس
invertible	معکوسپذیر
element	عنصر
quasi-regular	منتظم نمای
quotient	خارج قسمتی
ring	حلقهٔ
ring	حلقه
artinian	آرتینی
boolean	بولی
commutative	تعویضپذیر
discrete valuation	ارزیابی گسسته
division	بخشی
endomorphism	درونریختی
euclidean	اقلیدسی
extension	توسیع
group	گروه
integrally closed	به طور صحیح بسته
left quotient	خارج قسمتی چپ

local	موضعی
noetherian	نوتری
opposite	متقابل
primitive	اولیه
prime	اول
quotient	خارج قسمتی
radical	رادیکال
regular	منتظم
semiprime	نیمه اول
semisimple	نیمه ساده
simple	ساده
subdirectly irreducible	به طور زیر مستقیم تحویل ناپذیر
root	ریشه
multiple	چندگانه
of unity	واحد
simple	ساده
row	سطر (ی)
echelon form	شکل . . . پلکانی
elementary operation	مقدماتی عمل
rank	رتبه
space	فضای
vector	بردار
ruler	خط کش

scalar	اسکالر
matrix	ماتریس
second isomorphism	دوم یکریختی
theorem	قضیهٔ
secondary	ثانوی
matrix	ماتریس
semidirect	نیمه مستقیم
product	حاصل ضرب
semigroup	نیمگروه
semiprime	نیمه اول
ring	حلقهٔ
semisimple	نیمه ساده
module	مدول
ring	حلقهٔ
separable	جدایی پذیر (ی)
degree	درجهٔ
element	عنصر
extension	توسیع
polynomial	چند جمله‌ای
separably	به طور جدایی پذیر
generated	تولید شده
extension	توسیع
separating	جداگر
transcendence	تعالی
base	پایهٔ

sequence	دنباله
exact	کامل
short	کوتاه
series	سری (ها)
ascending	افزایشی
central	مرکزی
composition	ترکیب
equivalent	معادل
formal power	توانی صوری
normal	نرمال
solvable	حلپذیر
subnormal	زیرنرمال
set (s)	مجموعه (ها)
denumerable	شمارشپذیر
disjoint	از هم جدا
empty	تهی
equipollent	همتوان
finite	متناهی
infinite	نامتناهی
linearly	خطی
ordered	مرتب
multiplicative	ضربی
null	پوچ
partially	جزئی
ordered	مرتب

power	توان
underlying	زمینه
well ordered	خوش ترتیب
short	کوتاه
exact	کامل
sequence	دنبالهٔ
five	پنج
lemma	لم
sign	علامت
of a permutation	یک جایگشت
similar	متشابه
matrices	ماتریسهای
simple	ساده
component	مؤلفهٔ
extension	توسیع
field	میدان
group	گروه
module	مدول
ordering	ترتیب
ring	حلقهٔ
root	ریشهٔ
singleton	یکانی
skew-symmetric	متقارن اریب
matrix	ماتریس
multilinear	چند خطی

form	فرم
solvable	حلپذیر
by radicals	به وسیلهٔ رادیکالها
group	گروه
series	سری
span	پیما
spectrum	طیف
split	تجزیه
exact	کامل
sequence	دنبالهٔ
splitting	تجزیه گر
field	میدان
stabilizer	پایدارساز
stable	پایدار
intermediate	میانی
field	میدان
standard	متعارف
n-product	n - حاصل ضرب
subalgebra	زیر جبر
subclass	زیر رده
subdirect	زیر مستقیم
product	حاصل ضرب
subdirectly	به طور زیر مستقیم
irreducible	تحویل ناپذیر
ring	حلقهٔ

subfield (s)	زیر میدان (ها)
composite	ترکیب
linearly	به طور خطی
disjoint	از هم جدا
maximal	ماکزیمال
prime	اول
subgroup	زیر گروه
characteristic	مشخص
closed	بسته
commutator	تعویضگر
cyclic	دوری
derived	مشتق
fully	کاملاً
invariant	پایا
join of	الحاق
maximal	ماکزیمال
normal	نرمال
minimal	مینیمال
normal	نرمال
normal	نرمال
proper	حقیقی
transitive	متعدی
trivial	بدیهی
submodule	زیرمدول
generated	باتولید

finitely	متناهی
subnormal	زیر نرمال
series	سری
subring	زیر حلقه
subset	زیر مجموعه
subspace	زیر فضا
ϕ-invariant	ϕ-پایا
substitution	جانشانی
homomorphism	همریختی
successor	تالی
immediate	بلافصل
sum (= coproduct)	مجموع (= هم حاصل ضرب)
direct	مستقیم
summand	جمعوند
direct	مستقیم
surjective	سورژکتیو
function	تابع
symmetric	متقارن
group	گروه
matrix	ماتریس
multilinear	چند خطی
function	تابع
rational	گویا
function	تابع
relation	رابطهٔ

tensor	تانسور (ی)
product	ضرب
terminal	نهایی
object	شیء
third isomorphism	سوم یکریختی
theorem	قضیهٔ
torsion	تاب (ی)
group	گروه
module	مدول
subgroup	زیرگروه
submodule	زیرمدول
torsion-free	فارغ از تاب
group	گروه
module	مدول
total	کل
degree	درجهٔ
ordering	ترتیب
trace	اثر
transcendence	تعالی
base	پایهٔ
degree	درجهٔ
separating	جداگر
base	پایهٔ
transcendental	متعالی
element	عنصر

extension	توسیع
purely	صرفاً
extension	توسیع
transfinite	ترانسفینی
induction	استقرای
transformation	تبدیل
linear	خطی
natural	طبیعی
transitive	تعدی
relation	رابطهٔ
subgroup	زیرگروه
subring	زیر حلقهٔ
translation	انتقال
transpose	ترانهاده
of a matrix	یک ماتریس
transposition	ترانهش
triangular	مثلثی
matrix	ماتریس
trichotomy	تثلیث
law	قانون
trivial	بدیهی
ideal	ایده‌آل
underlying	زمینه
set	مجموعهٔ

union	اجتماع
disjoint	از هم جدا
unique	یکتایی
factorization	تجزیه
domain	دامنهٔ
unit	یکه
map	نگاشت
unitary	یکانی
module	مدول
unity	واحد
root (of)	ریشهٔ
primitive	اولیهٔ
universal	عمومی
element	عنصر
mapping	نگاشت
property	خاصیت
object	شیء
upper	بالایی
bound	کران
valuation	ارزیابی
domain	دامنهٔ
discrete	گسسته
ring	حلقهٔ
variety	واریته

vector	بردار (ی)
column	ستونی
row	سطری
space	فضای
finite dimensional	بابعد متناهی
weak	ضعیف
direct	مستقیم
product	حاصل ضرب
well ordered	خوش ترتیب
set	مجموعهٔ
well ordering	خوش ترتیبی
law of	قانون
principle	اصل
word	کلمه
reduced	تحویل یافته
empty	تهی
zero	صفر
divisor	مقسوم علیه
element	عنصر
matrix	ماتریس
morphism	ریخت
object	شیء

فهرست راهنما